BiPAC 7401VGP *R3*

VoIP/ 802.11g ADSL2+ Firewall Router

User Manual

Version released: 6.24b.dm2

Last Revised Date: July 04, 2012

Table of Contents

Chapter 1: Introduction 1
Introduction to your Router 1
Features 1
Chapter 2: Installing the Router 1
Important note for using this router 1
Package Contents 1
Device Description 2
Cabling 4
Chapter 3: Basic Installation 5
Connecting Your Router 6
Factory Default Settings 15
Information from your ISP 16
Configuring with your Web Browser 17
Chapter 4: Configuration 18
Status 19
ADSL Status 19
EWAN Status 21
ARP Table 21
DHCP Table 22
Routing Table 23
NAT Sessions 24
UPnP Portmap 24
VoIP Status 24
VoIP Call Log 25
Event Log 26
Error Log 27
IDS Log 27
Diagnostic 27
Quick Start 28
Configuration 34
LAN - Local Area Network 35
Bridge Interface 35
Ethernet 36
IP Alias 37
IPv6 Autoconfig 38
Ethernet Client Filter 39
Wireless 40
Wireless Security 42
Wireless Client / MAC Address Filter 44
WPS 46
Port Setting 58
DHCP Server 59
WAN - Wide Area Network 60
System 78
Time Zone 78
Remote Access 79
Firmware Upgrade 79
Backup / Restore 80
Restart Router 81
User Management 82
Mail Alert 84
Firewall and Access Control 85

General Settings 86
Packet Filter 88
Intrusion Detection 94
URL Filter 96
IM / P2P Blocking 99
Firewall Log 100
VoIP - Voice over Internet Protocol 101
SIP Device Parameters 102
SIP Accounts 105
Phone Port 106
PSTN Dial Plan (Router with LINE port only) 108
VoIP Dial Plan 112
Call Feature 115
Speed Dial 115
Ring & Tone 116
QoS - Quality of Service 119
Prioritization 119
Outbound IP Throttling (LAN to WAN) 121
Inbound IP Throttling (WAN to LAN) 122
Virtual Server (known as Port Forwarding) 128
Add Virtual Server 129
Edit DMZ Host 131
Edit One-to-One NAT (Network Address Translation) 132
Wake on LAN 135
Time Schedule 136
Configuration of Time Schedule 137
Advanced 139
Static Route 139
Static ARP 139
Dynamic DNS 140
Device Management 141
IGMP 145
MLD 145
VLAN Bridge 146
Logout 147
Chapter 5: Troubleshooting 148
Appendix: Product Support & Contact 150

Chapter 1: Introduction

Introduction to your Router

Welcome to the VoIP/ 802.11g ADSL2+ Firewall Router. The router is an “all-in-one” VoIP ADSL router, combining an ADSL modem, ADSL router, Ethernet network switch and 1 port for Voice over IP functionalities, providing everything you need to get the machines on your network connected to the Internet over your ADSL broadband connection. With features such as a Quick-Start wizard and DHCP Server, you can be online in no time at all and with a minimum of fuss and configuration, catering for first-time users to the guru requiring advanced features and control over their Internet connection and network.

Features

Express Internet Access

The router complies with ADSL worldwide standards. It supports downstream rate up to 12/24 Mbps with ADSL2/2+, 8Mbps with ADSL. Users enjoy not only high-speed ADSL services but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (ITU G.992.1); G.lite (ITU G.992.2); G.hs (ITU G994.1); G.dmt.bis (ITU G.992.3); G.dmt.bis.plus (ITU G.992.5)).

Voice over IP compliance with SIP standard

The router supports cost-effective, toll-quality voice calls over the Internet. It complies with the most popular industrial standard, SIP protocol, to ensure the interoperability with SIP devices and major VoIP Gateways. The VoIP router supports call waiting, silence suppression, voice activity detection (VAD), comfort noise generation (CNG), line echo cancellation, caller ID (Bell 202, V3) and so on.

802.11g Wireless AP with WPA Support (Wireless Router only)

With integrated 802.11g Wireless Access Point in the router, the device offers a quick and easy access among wired network, wireless network and broadband connection with single device simplicity, and as a result, mobility to the users. In addition to 54 Mbps 802.11g data rate, it also interoperates backward with existing 802.11b equipment. The Wi-Fi Protected Access (WPA-PSK and WPA2-PSK) and Wired Equivalent Privacy (WEP) supported features enhance the security level of data protection and access control via Wireless LAN.

Fast Ethernet Switch

A 4-port 10/100Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports. An Ethernet straight or crossover cable can be used directly for auto detection.

EWAN

Besides using ADSL to get connected to the Internet, the router offers its Ethernet port 1 as a WAN port to be used to connect to Cable Modems, VDSL and fibre optic lines. This alternative, yet faster method to connect to the internet will provide users more flexibility to get online.

Dual WAN

Dual WAN is a new way of getting connected to the internet which is to use two of the ADSL/EWAN to deal with the unexpected case and balance traffic load. That is a way of improving greatly the robustness.

Multi-Protocol to Establish a Connection

It supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation overATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.

Quick Installation Wizard

It supports a WEB GUI page to install this device quickly. With this wizard, end users can enter the information easily which they get from their ISP, then surf the Internet immediately.

Universal Plug and Play (UPnP) and UPnP NAT Traversal

This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.

Network Address Translation (NAT)

Allows multi-users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.

SOHO Firewall Security with DoS and SPI

Along with the built-in NAT natural firewall feature, the router also provides advanced hacker pattern-filtering protection. It can automatically detect and block Denial of Service (DoS) attacks. The router is built with Stateful Packet Inspection (SPI) to determine if a data packet is allowed through the firewall to the private LAN.

Domain Name System (DNS) Relay

It provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in the outside network.

Dynamic Domain Name System (DDNS)

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from a DDNS service like http://www.dyndns.org/. More than 5 DDNS servers are supported.

Quality of Service (QoS)

QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets, customer information, or management information move through the router ay lightning speed, even under heavy load. The QoS features are configurable by source IP address, destination IP address, protocol, and port. You can throttle the speed at which different types of outgoing data pass through the router, to ensure P2P users don't saturate upload bandwidth, or office browsing doesn't bring client web serving to a halt. In addition, or alternatively, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

IPv6 supported

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4.

IPv6 has a vastly larger address space than IPv4. This results from the use of a 128-bit address, whereas IPv4 uses only 32 bits. The new address space thus supports 2128 (about 3.4×1038) addresses. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

IPv6 also implements new features that simplify aspects of address assignment (stateless address autoconfiguration) and network renumbering (prefix and router announcements) when changing Internet connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from Link Layer media addressing information (MAC address).
Network security is integrated into the design of the IPv6 architecture. Internet Protocol Security (IPsec) was originally developed for IPv6, but found widespread optional deployment first in IPv4 (into which it was back-engineered). The IPv6 specifications mandate IPsec implementation as a fundamental interoperability requirement.

Virtual Server ("port forwarding")

Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it. For example, a user can assign a PC in the LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse inside web servers directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.

Rich Packet Filtering

Not only filters the packet based on IP address, but also based on Port numbers. It will filter packets from and to the Internet, and also provides a higher level of security control.

Dynamic Host Configuration Protocol (DHCP) Client and Server

In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

Static and RIP1/2 Routing

It has routing capability and supports easy static routing table or RIP1/2 routing protocol.

Simple Network Management Protocol (SNMP)

It is an easy way to remotely manage the router via SNMP.

Web based GUI

It supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.

Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI.

Rich Management Interfaces

It supports flexible management interfaces with local console port, LAN port, and WAN port. Users can use terminal applications through the console port to configure and manage the device, or Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage the device.

Chapter 2: Installing the Router

Important note for using this router

Warning

- Do not use this router in a high humidity or high temperature environment.
- Do not apply the same power source for this router to other types of equipments.
- Do not open or repair the case yourself. If the device becomes too hot, turn it off immediately and have it repaired at a qualified service center.
- Avoid using this product and all its accessories outdoor.

Attention

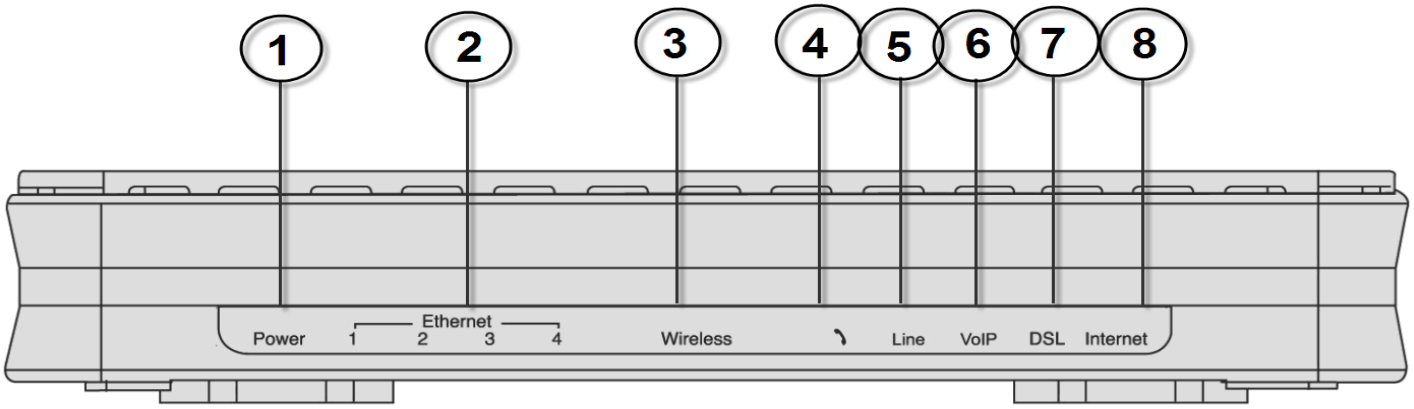
- Place the router on a stable surface.
- Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the router.

Package Contents

- **VoIP/ 802.11g ADSL2+ Firewall Router**
- **CD-ROM containing the online manual**
- **RJ-11 ADSL/telephone Cable**
- **Ethernet (CAT-5) Cable**
- **RJ-45 to RS-232 Console Kit**
- **Power adapter**
- **A detachable antenna (Wireless Model only)**
- **Quick Start Guide**
- **Splitter/ Micro-filter (Optional)**

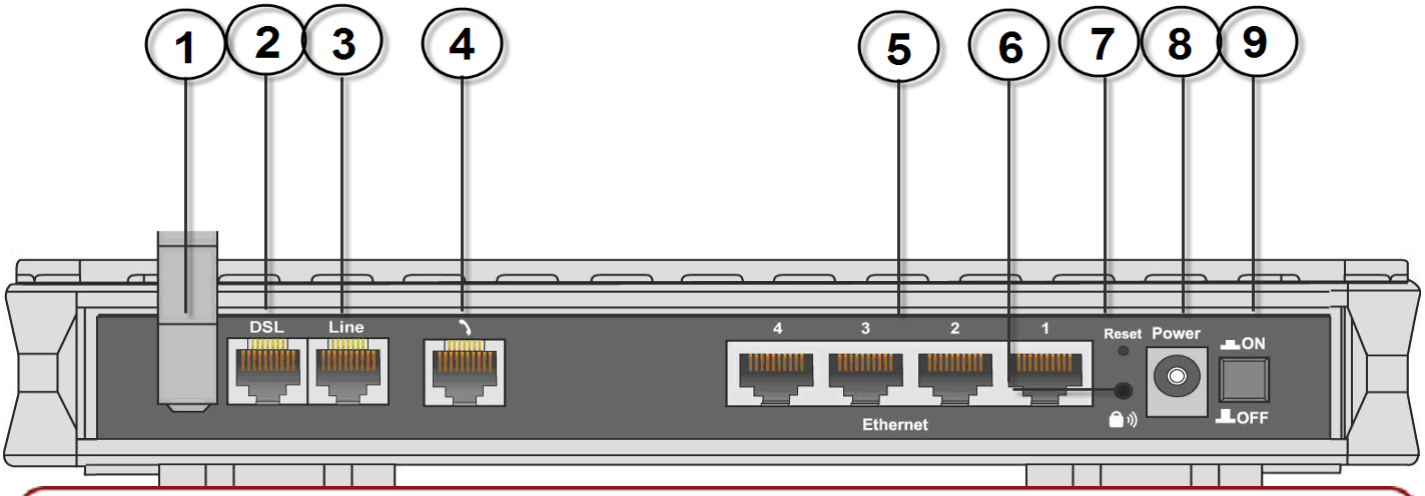
Device Description

The Front LEDs



Port		Meaning
1	**Power**	Both red and green LEDs lit together when power is ON. Lit red means system failure. Restart the device or contact support. Lit green when the device is ready.
2	**Ethernet Port**	Lit when one of LAN ports is connected to an Ethernet device. Lit green when the speed of transmission hits 100Mbps; Lit orange when the speed of transmission hits 10Mbps. Blink when data is being Transmitted / Received.
3	**Wireless**	Lit green when the wireless connection is established. Flash when sending/receiving data. Flash once per second while wi-fi protected setup is in progress.
4	**Phone (RJ-11 connector)**	Lit green when phone is off hook.
5	**Line(Router with LINE port only)**	Lit green when the inbound and outbound calls are transmitted through PSTN.
6	**VoIP(RJ-11 connector)**	Lit when the SIP Registration is OK. Green for Phone.
7	**DSL**	Lit Green when the device is successfully connected to an ADSL DSLAM. (“line sync”).
8	**Internet**	Lit red when WAN port fails to get IP address. Lit green when WAN port gets IP address successfully. Lit off when the device is in bridge mode or when WAN connection is absent.

The Rear Ports



NOTE: Ethernet # 4 can be used as a console port. You need a special console tool which is included in the package to connect with the LAN.

Port		Meaning
1	**Antenna**	Connect the detachable antenna to this port.
2	**DSL**	Connect this port to the ADSL/telephone network with the RJ-11 cable (telephone) provided.
3	**Line**	Connect this port to the telephone jack on the wall with RJ-11cable.
4	**Phone**	Connect this port to an analog phone set with RJ-11 cable.
5	**Ethernet**	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps. ***Caution: Port 4 can be either a LAN or Console port at a time but not both.***
6	**WPS**	Push WPS button for less than 5 sec to trigger Wi-Fi Protected Setup function; push WPS button for more than 5 sec to enable/disable WLAN Service.
7	**RESET**	To be sure the device is being turned on press RESET button for: 1-3 seconds: quick reset the device. 6 seconds and above, power off, power on the device: restore to factory default settings. (Cannot login to the router or forgot your Username/Password. Press the button for more than 6 seconds). ***Caution: After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device again.***
8	**Power**	Connect it with the supplied power adapter.
9	**Power Switch**	Power ON/OFF switch.

Cabling

One of the most common causes of problem is bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front panel of your router is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify if you are using the proper cables.

Make sure that all devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line as your router have a line filter connected between them and the wall outlet (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and that all line filters are correctly installed in a right way. If line filter is not installed and connected properly, it may cause problem to your ADSL connection or may result in frequent disconnections.

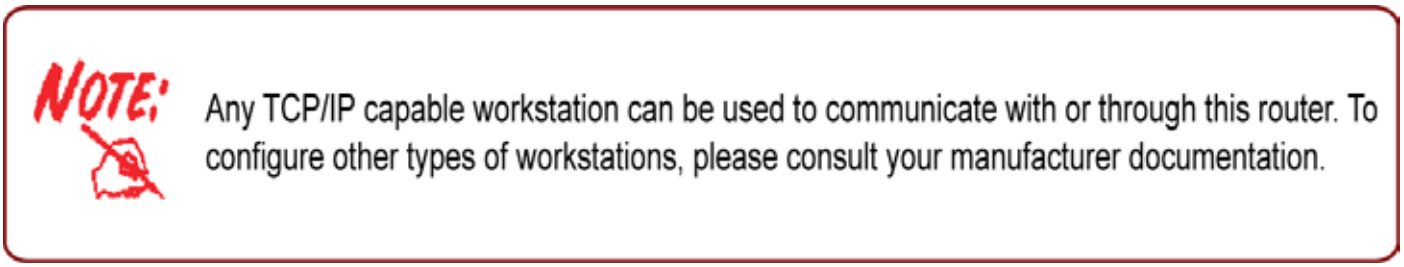
Chapter 3: Basic Installation

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

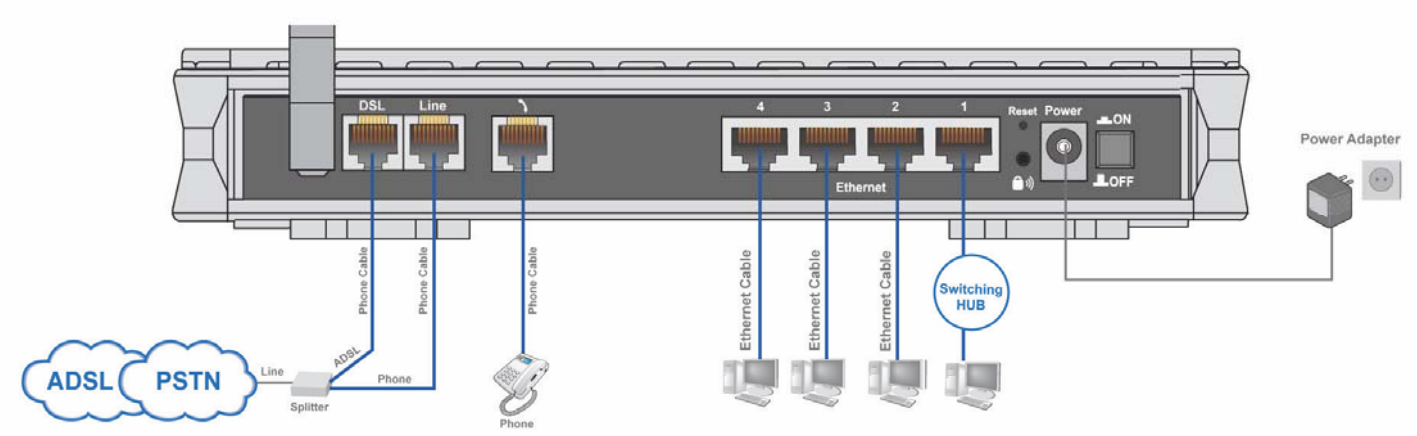
There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.1.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

Please follow the following steps to configure your PC network environment.


NOTE:
Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

Connecting Your Router

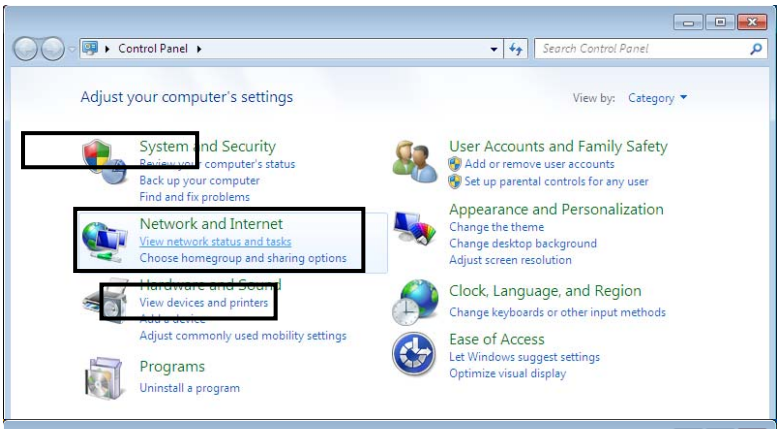
1. Connect this router to a **LAN** (Local Area Network) and the ADSL/telephone (**ADSL**) network.
2. Power on the device.
3. Make sure the **Power LED** lit steadily and that the **LAN** LED is lit.
4. Connect your router to the telephone jack on the wall with RJ-11 cable.



Network Configuration

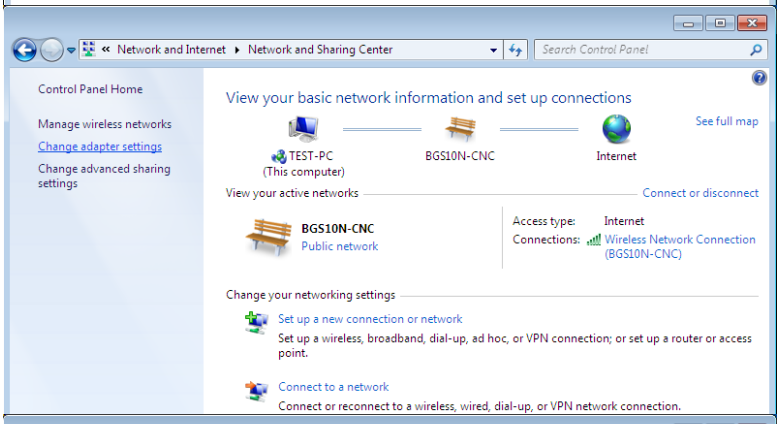
Configuring PC in Windows 7

1 Go to Start. Click on Control Panel.

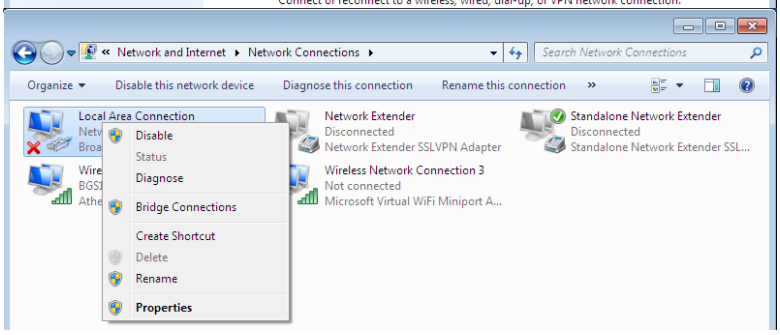


2. Then click on Network and Internet.

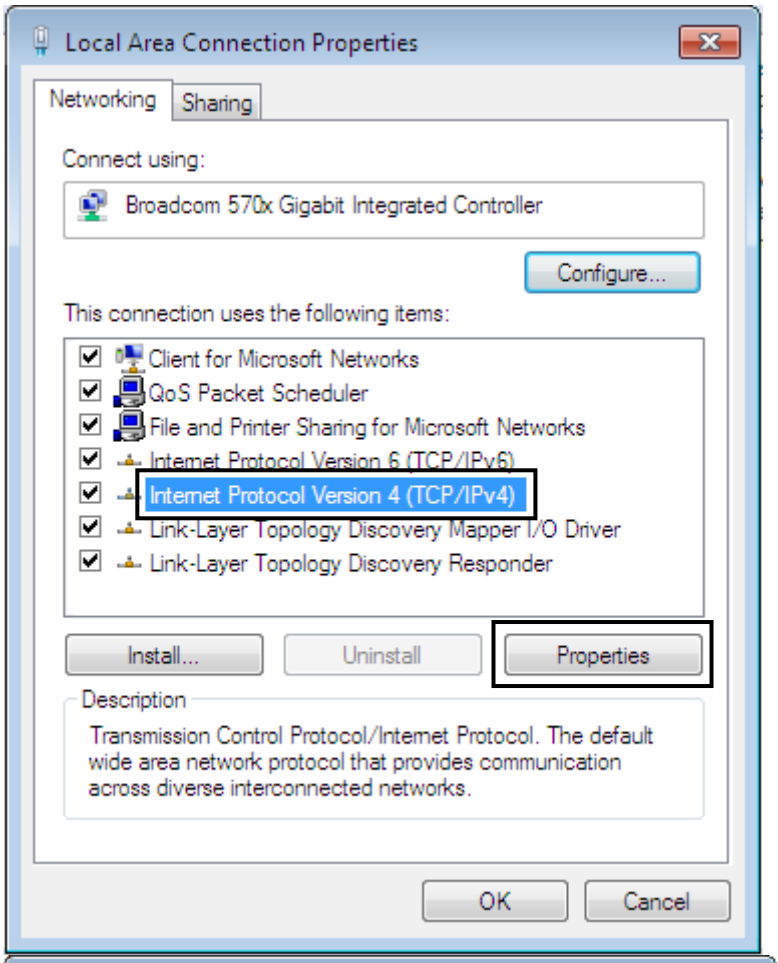
3. When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.


Network and Internet
Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
TEST-PC
(This computer)
BGS10N-CNC
Internet
View your active networks
Connect or disconnect
BGS10N-CNC
Public network
Access type: Internet
Connections: Wireless Network Connection (BGS10N-CNC)
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

4. Select the Local Area Connection, and right click the icon to select Properties.

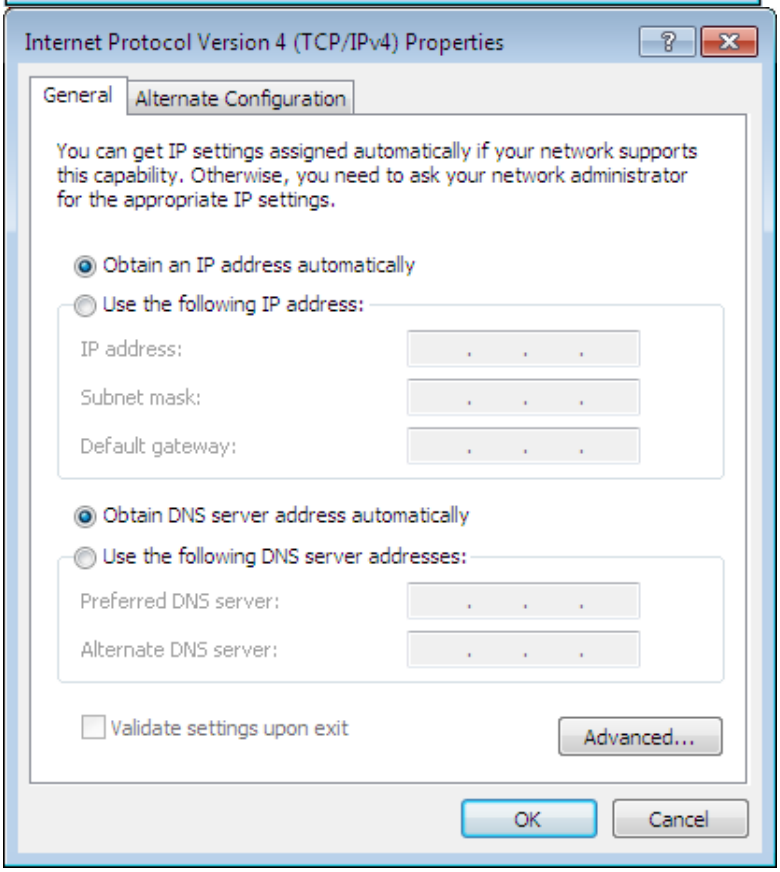


5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



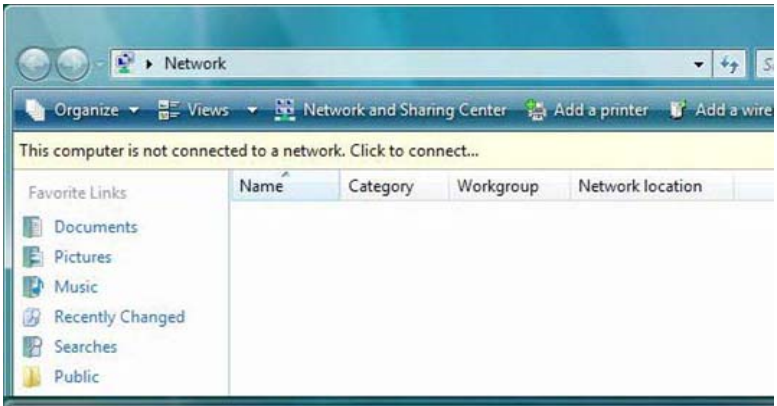
6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.

7. Click OK again in the Local Area Connection Properties window to apply the new configuration.

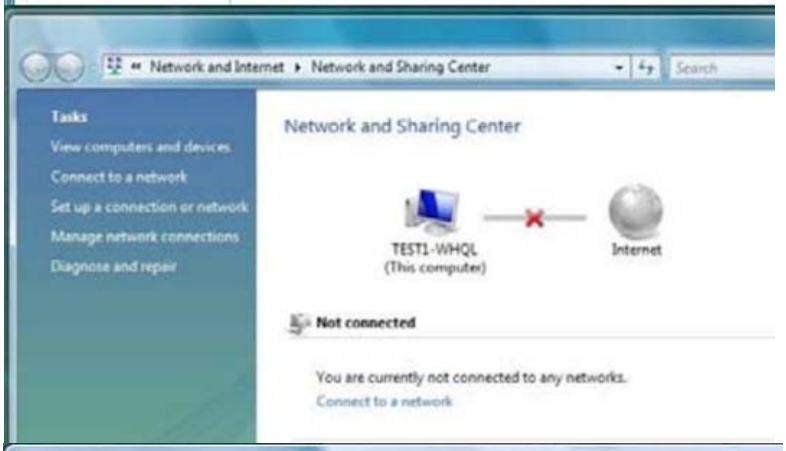

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Configuring PC in Windows Vista

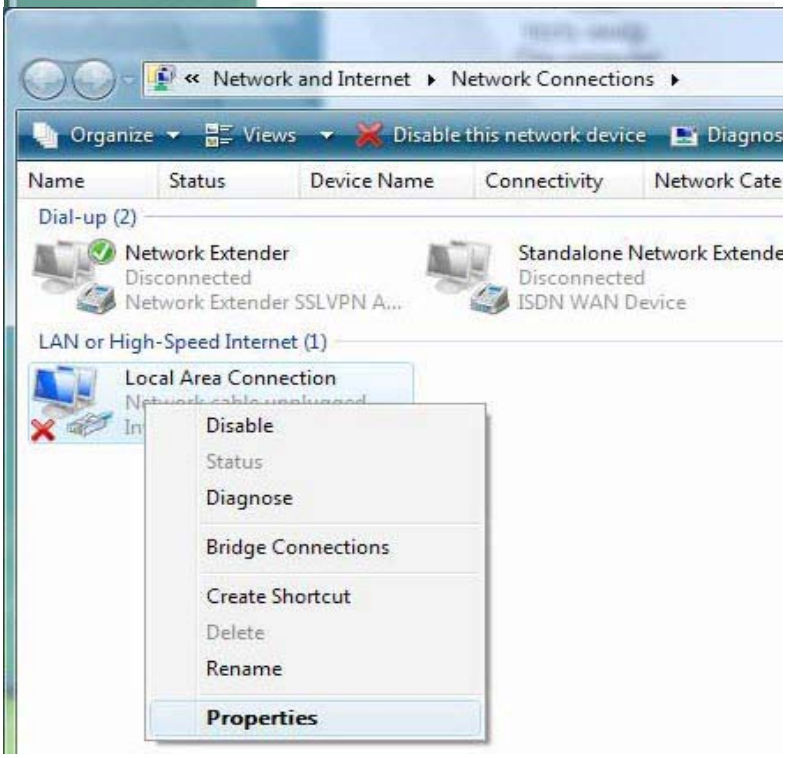
1. Go to Start. Click on Network.
2. Then click on Network and Sharing Center at the top bar.



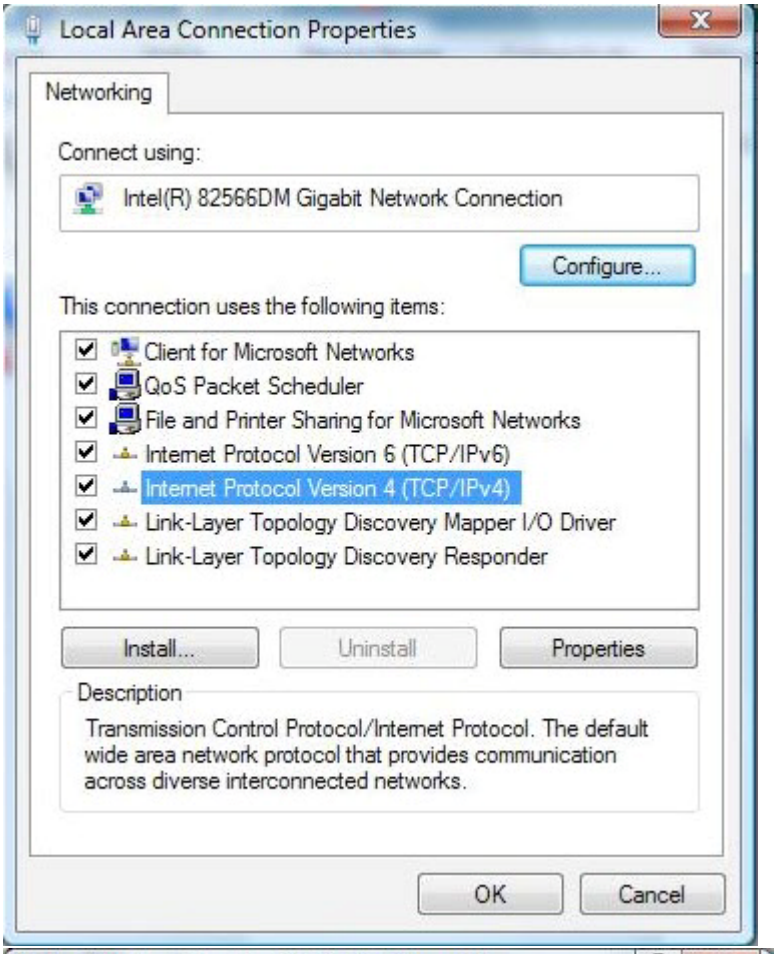
3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.



4. Select the Local Area Connection, and right click the icon to select Properties.

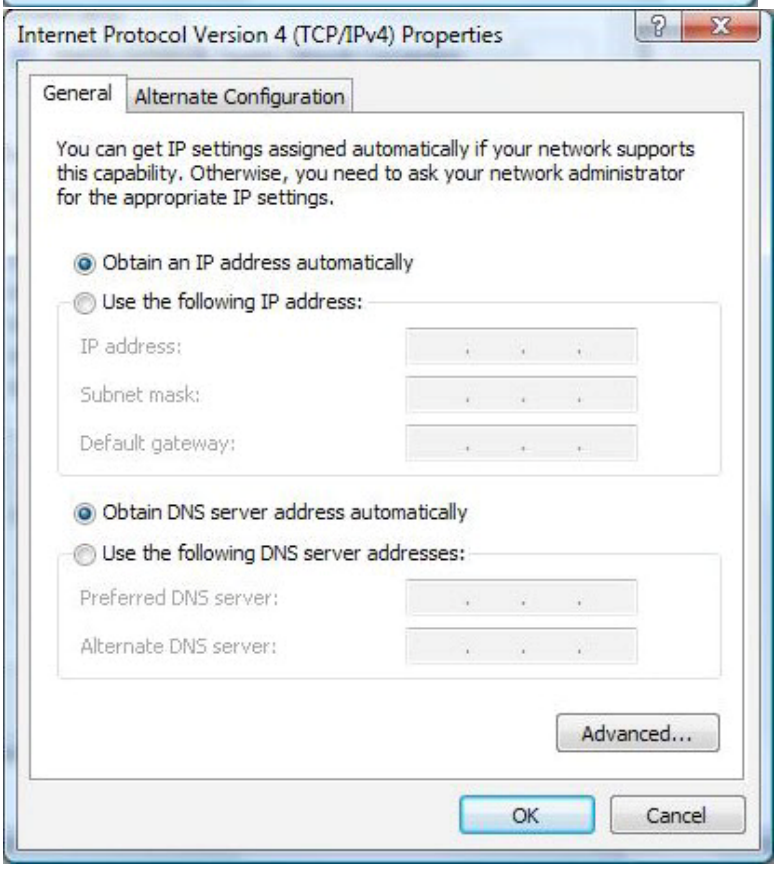


5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the set- ting.

7. Click OK again in the Local Area Connection Properties window to apply the new configuration.

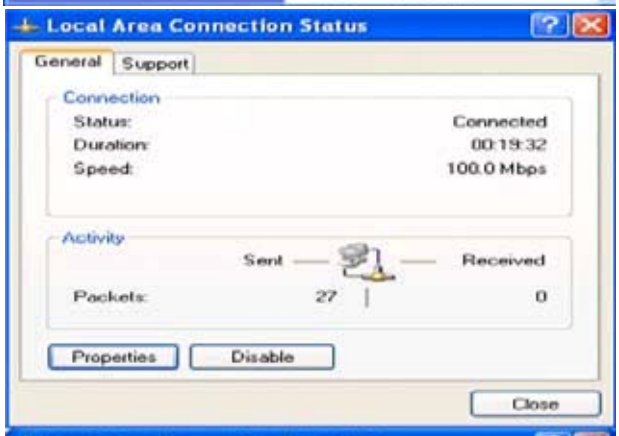

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Configuring PC in Windows XP

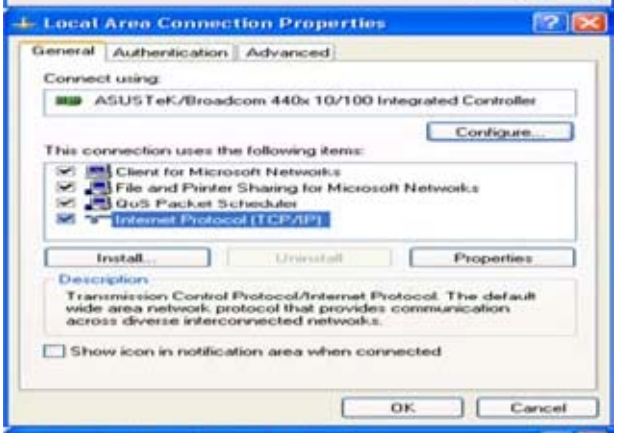
1. Go to Start > Control Panel (in Classic View). In the Control Panel, double-click on Network Connections.

2. Double-click Local Area Connection.

3. In the Local Area Connection Status window, click Properties.

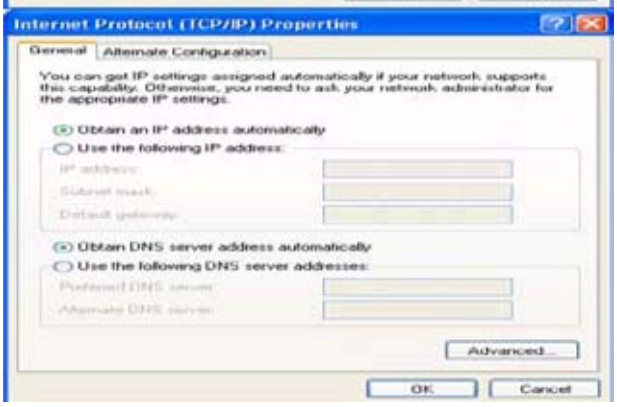


4. Select Internet Protocol (TCP/IP) and click Properties.


Local Area Connection Properties
General Authentication Advanced
Connect using:
ASUSTeK/Broadcom 440x 10/100 Integrated Controller
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

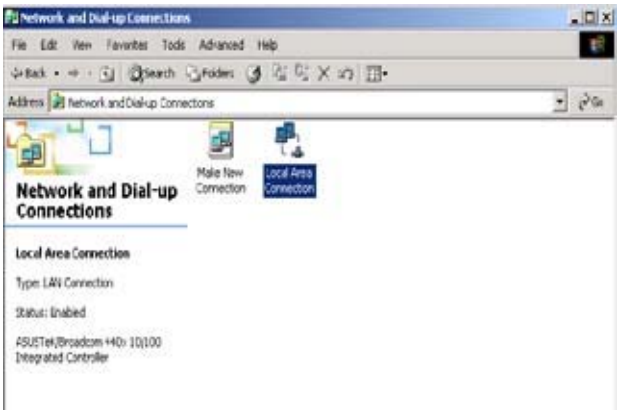
5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.

6. Click OK to finish the configuration.


Internet Protocol (TCP/IP) Properties
General Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK Cancel

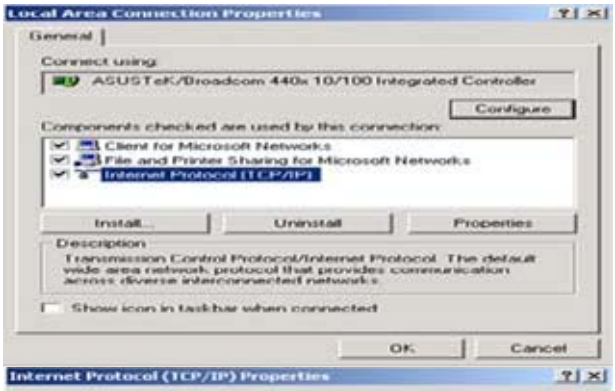
Configuring PC in Windows 2000

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.
2. Double-click Local Area Connection.

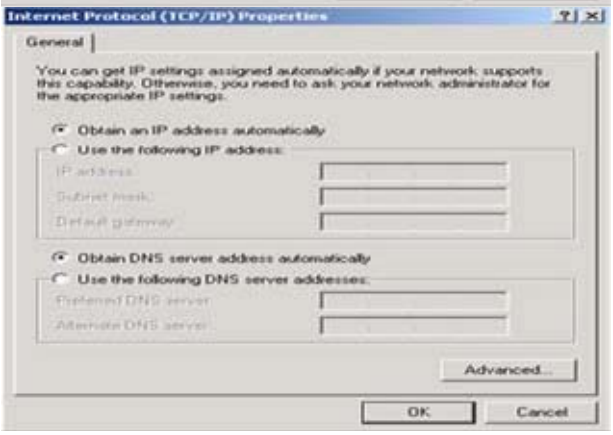


3. In the Local Area Connection Status window click Properties.

4. Select Internet Protocol (TCP/IP) and click Properties.

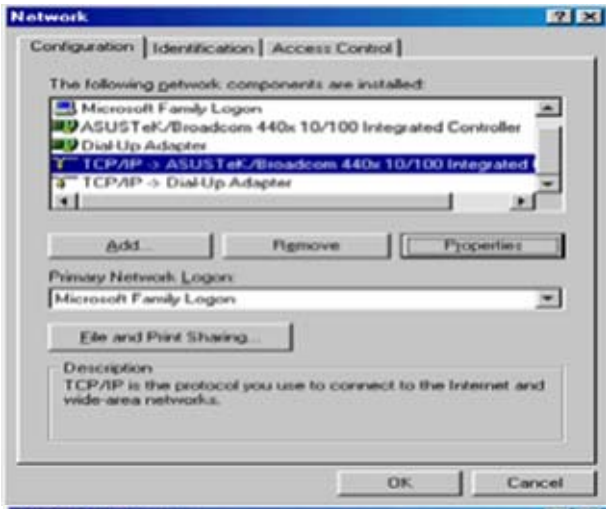


5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

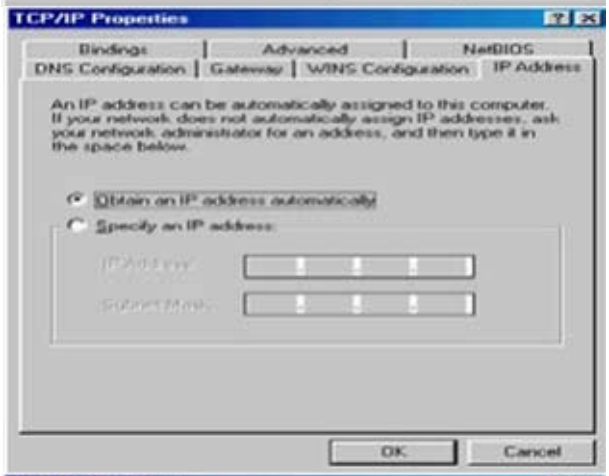

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Configuring PC in Windows 95/98/Me

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.
2. Select TCP/IP > NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.



3. Select the Obtain an IP address automatically radio button.

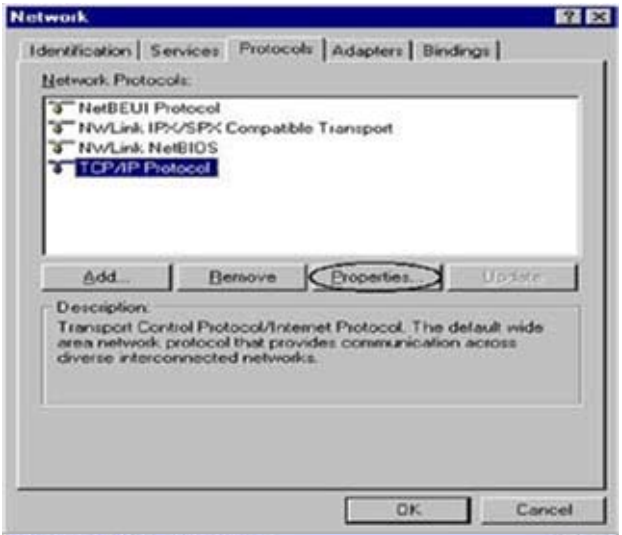

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
OK
Cancel

4. Then select the DNS Configuration.
5. Select the Disable DNS radio button and click OK to finish the configuration.

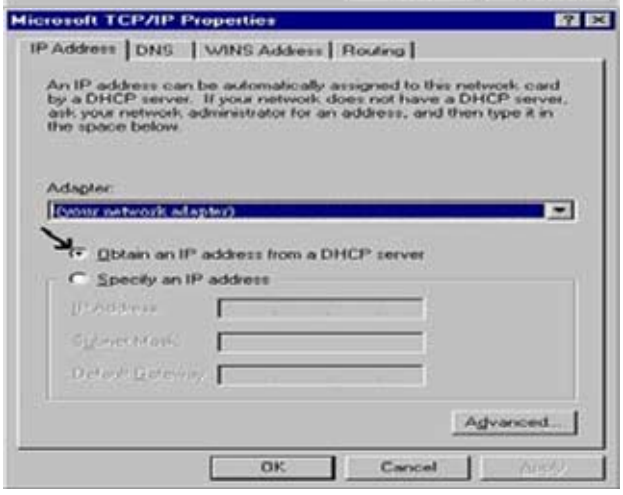
Configuring PC in Windows NT4.0

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.

2. Select TCP/IP Protocol and click Properties.



3. Select the Obtain an IP address from a DHCP server radio button and click OK.


Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
[your network adapter]
Obtain an IP address from a DHCP server
Specify an IP address
Advanced...
OK
Cancel

Factory Default Settings

Before configuring your router, you need to know the following default settings.

Web Interface (Username and Password)

- Username: admin
- Password: admin

Attention

If you ever forget the login password, please press the reset button for more than 6 seconds to restore the factory default setting.

The default username and password are “**admin**” and “**admin**” respectively.

Device LAN IP settings

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0

ISP setting in WAN site

- PPPoE

DHCP server

- DHCP server is enabled.
- Start IP Address: 192.168.1.100
- IP pool counts: 100

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown in the table.

LAN Port		WAN Port
IP address	192.168.1.254	The PPPoE function is *enabled* to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled in ports 1, 2, 3 and 4	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP (Obtain an IP Address Automatically, Static IP (Fixed IP Address) or PPPoE.
Gather the information as illustrated in the following table and keep it for reference.

PPPoE (RFC2516)	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA (RFC2364)	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
MPoA (RFC1483/ RFC2684)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA (RFC1577)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
Pure Bridge	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.

Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click “Go”, a user name and password window prompt will appear. The default username and password are “admin” and “admin” respectively. (See Figure 3.14)

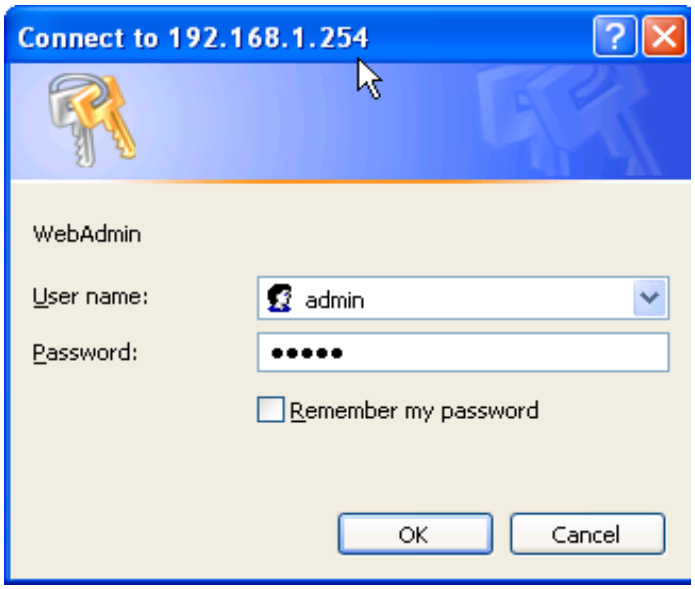


Figure 3.14: User name & Password Prompt Window

Congratulations!

You are now successfully logon to the VoIP/ 802.11g ADSL2+ Firewall Router!

Chapter 4: Configuration

At the configuration homepage, the left navigation column provides you the link to each configuration page. The category of each configuration page is listed as below.

Status

ADSL Status

EWAN Status

ARP Table

DHCP Table

Routing Table

NAT Sessions

UPnP Portmap

VoIP Status

VoIP Call Log

Event Log

Error Log

IDS Log

Diagnostic

Quick Start

Configuration

LAN

WAN

System

Firewall

VoIP

QoS

Virtual Server

Wake on LAN

Time Schedule

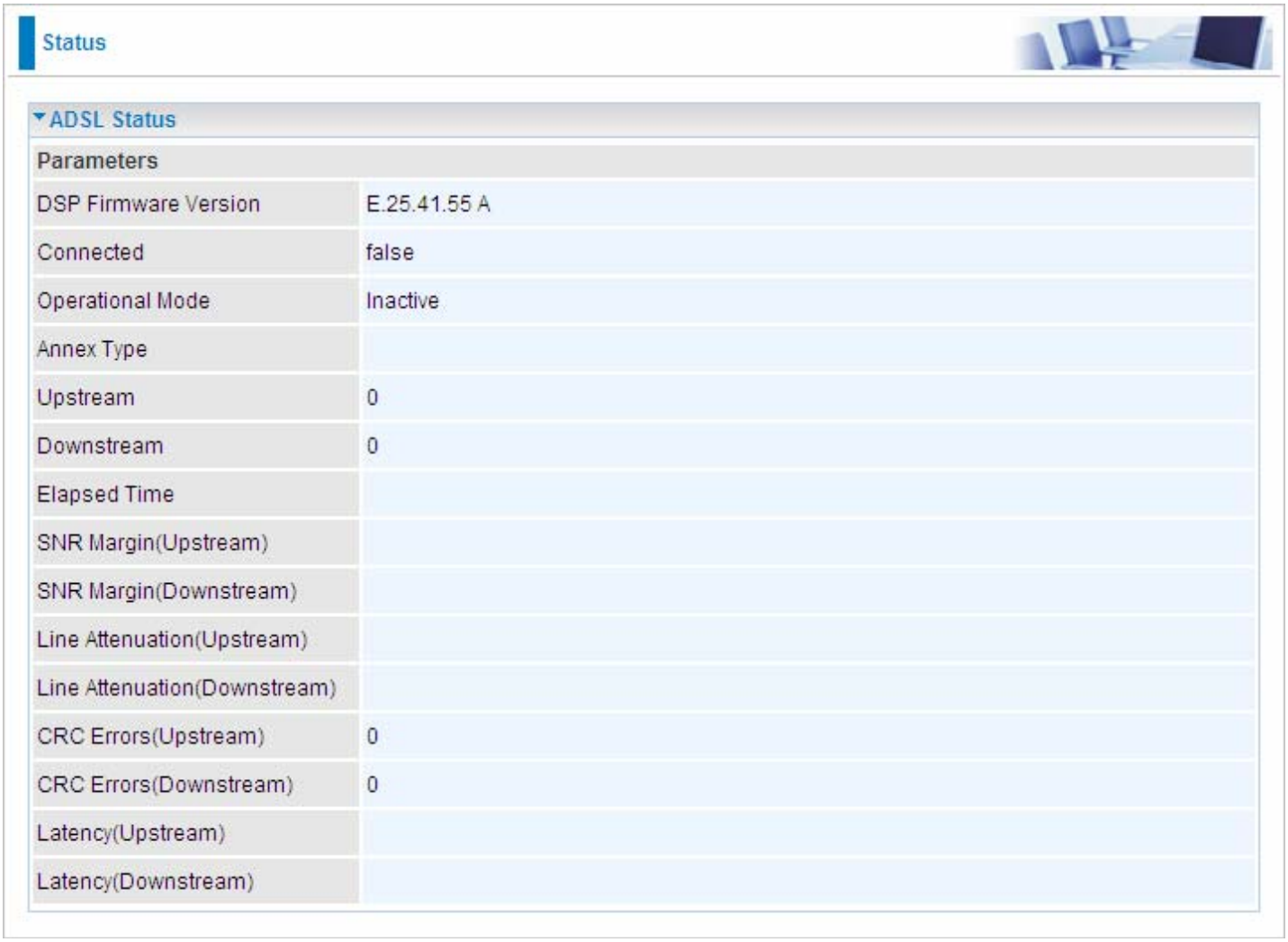
Advanced

Language (provides user interface in English and French languages)

Status

ADSL Status

This section displays the overall status of ADSL, such as DSP firmware version, Operational mode, Upstream/downstream rate, SNR margin, Line Attenuation, CRC Errors and Latency rate.



Parameters	
DSP Firmware Version	E.25.41.55 A
Connected	false
Operational Mode	Inactive
Annex Type	
Upstream	0
Downstream	0
Elapsed Time	
SNR Margin(Upstream)	
SNR Margin(Downstream)	
Line Attenuation(Upstream)	
Line Attenuation(Downstream)	
CRC Errors(Upstream)	0
CRC Errors(Downstream)	0
Latency(Upstream)	
Latency(Downstream)	

DSP Firmware Version: DSP code version.

Connected：To show if the ADSL line has already been connected.

Operational Mode: To show the state when user select “AUTO” on connect mode.

Annex Type: It is related to transmission rate, including Annex A and B.

Upstream: Upstream rate.

Downstream: Downstream rate.

Elapsed Time: It means the running time of ADSL.

SNR Margin (Upstream): This is noise margin in upstream.

SNR Margin (Downstream): This is noise margin in downstream.

Line Attenuation (Upstream): This is attenuation of signal in upstream.

Line Attenuation (Downstream): This is attenuation of signal in downstream.

CRC Errors (Upstream): This is CRC error in upstream.

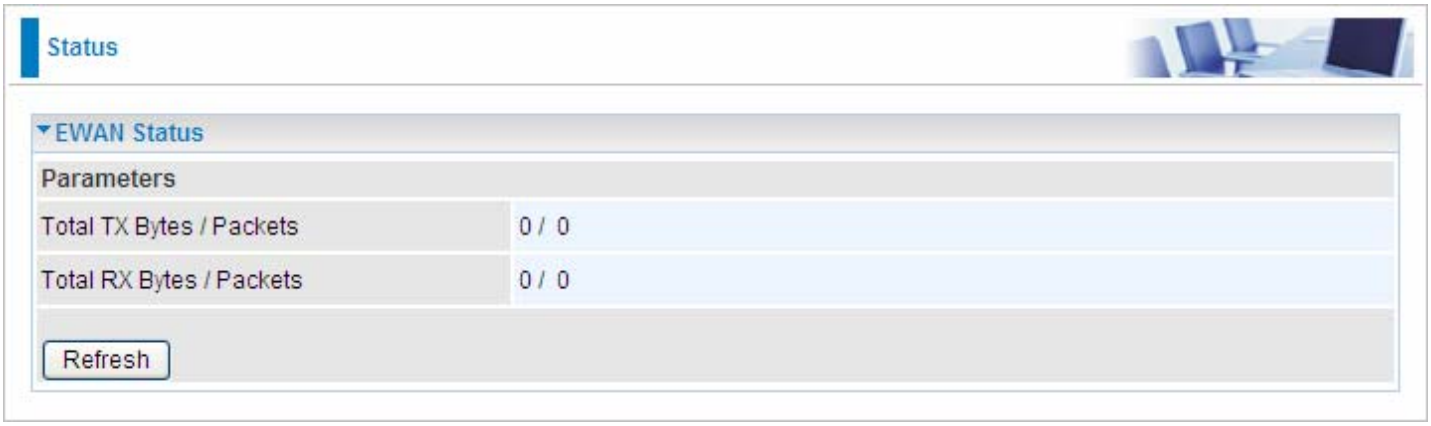
CRC Errors (Downstream): This is CRC error in downstream.

Latency (Upstream): This is time delay in downstream.

Latency (Upstream): This is time delay in upstream.

EWAN Status

Besides using ADSL to get connected to the Internet, the router offers its Ethernet port 1 as a WAN port to be used to connect to Cable Modems, VDSL and fiber optic lines. This alternative, yet faster method to connect to the internet will provide users more flexibility to get online.

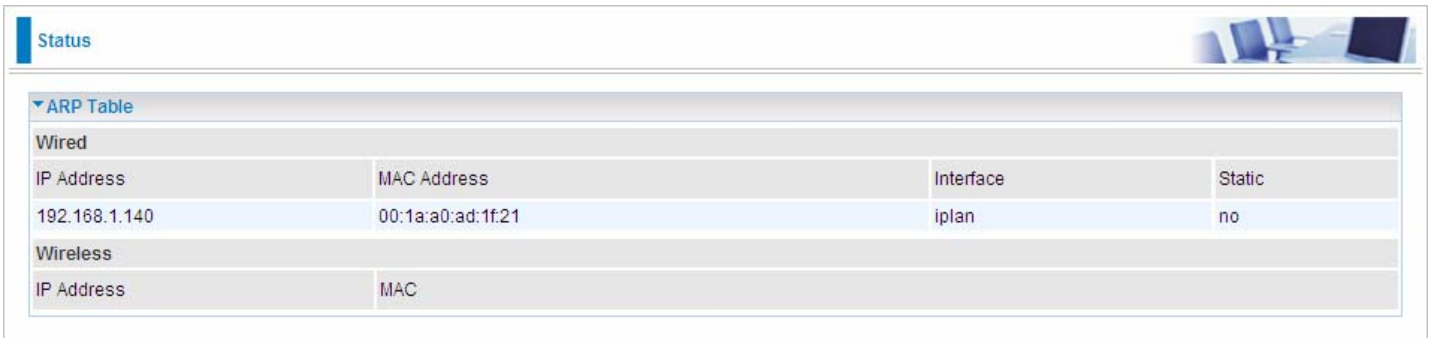


Total TX Bytes / Packets: The statistics of total data transmission in bytes / packets since system ready.

Total RX Bytes / Packets: The statistics of total data received in bytes / packets since system ready.

ARP Table

This section displays the router ARP (Address Resolution Protocol) Table which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is a quick way of determining the MAC address of the network interface of your PCs that use the Firewall – MAC Address Filter function. See the Firewall section of this manual for more information on this feature.



IP Address: Shows a list of IP addresses of devices on your LAN (Local Area Network).

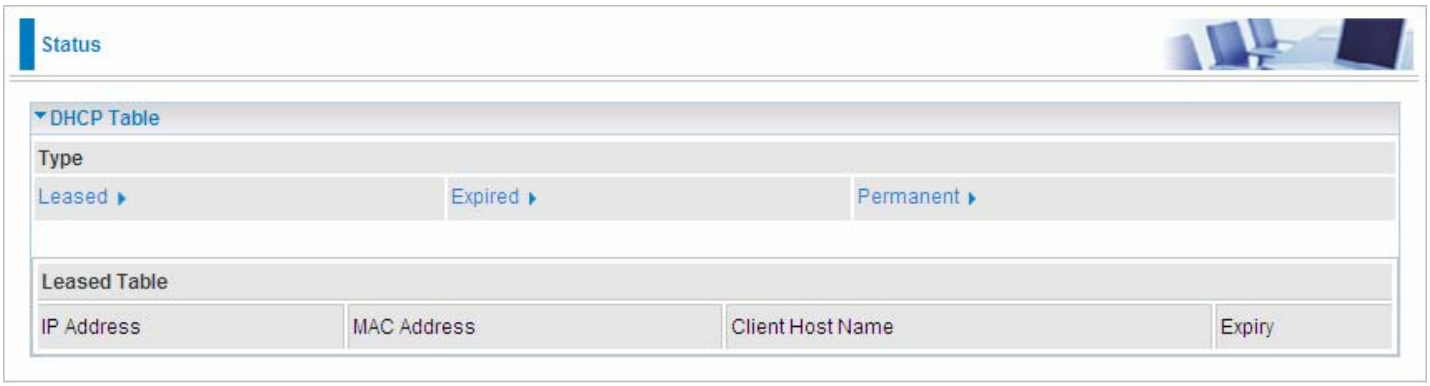
MAC Address: Shows the MAC (Media Access Control) addresses of each device on your LAN.

Interface: Shows the interface name (on the router) that this IP Address connects to.

Static: Static status of the ARP table entry:

"**no**" for dynamically-generated ARP table entries.
"**yes**" for static ARP table entries added by the user.

DHCP Table



Leased: Shows the information of the DHCP assigned IP addresses.

Expired: Shows the information of all expired IP addresses.

Permanent: Shows the fixed host mapping information.

Leased Table

IP Address: Shows the IP address that is assigned to each client.

MAC Address: Shows the MAC address of each client.

Client Host Name: Shows the Host Name (Computer Name) of the client.

Expiry: Shows the current lease time of each client.

Routing Table

Routing Table

Valid: A check mark indicates a successful routing status.

Destination: Shows the IP address of the destination network.

Netmask: Shows the destination Netmask address.

Gateway/Interface: Shows the IP address of the gateway or the existing interface that this route will use.

Cost: The number of hops counted as the cost of the route.

RIP Routing Table

Destination: Shows the IP address of the destination network.

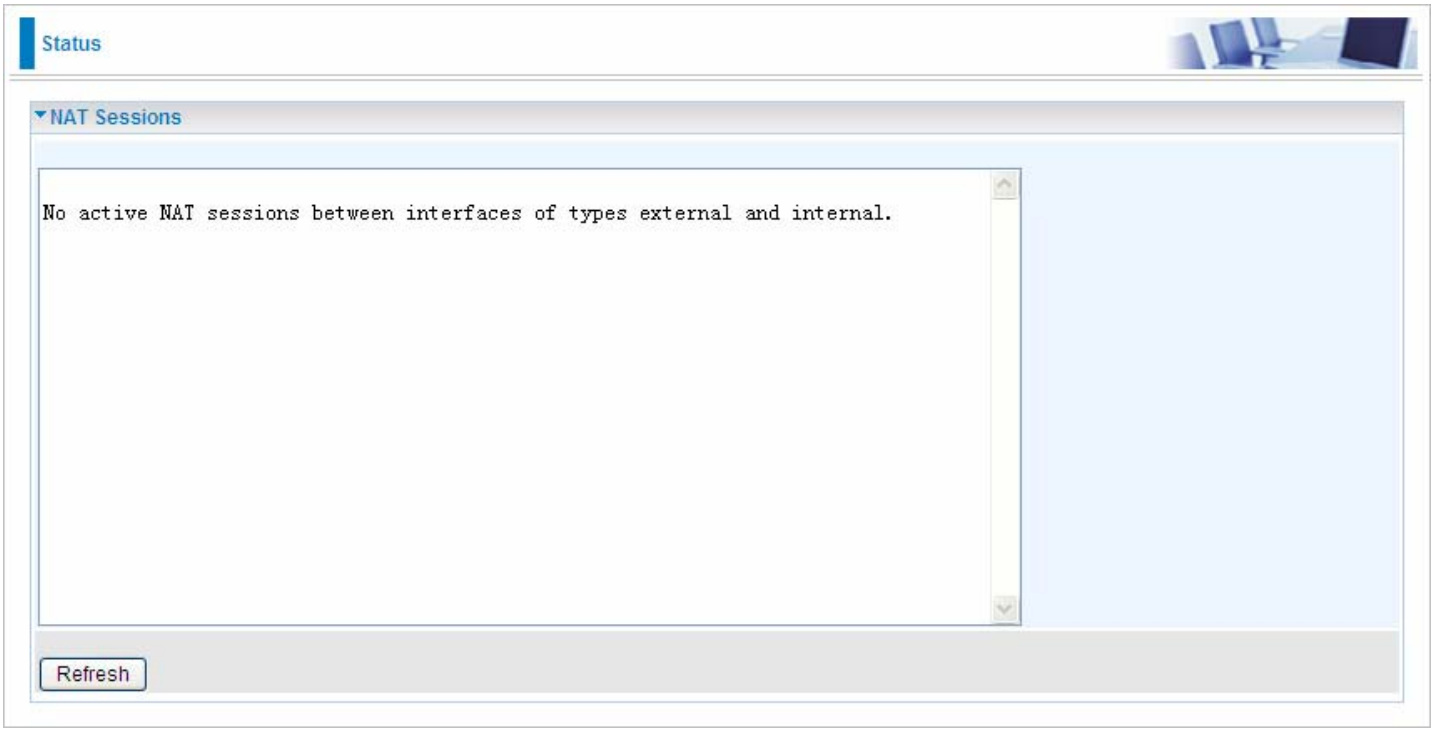
Netmask: Shows the destination Netmask address.

Gateway: Shows the IP address of the gateway that this route will use.

Cost: The number of hops counted as the cost of the route.

NAT Sessions

This section lists all the current NAT sessions between external (WAN) and internal (LAN) interface.

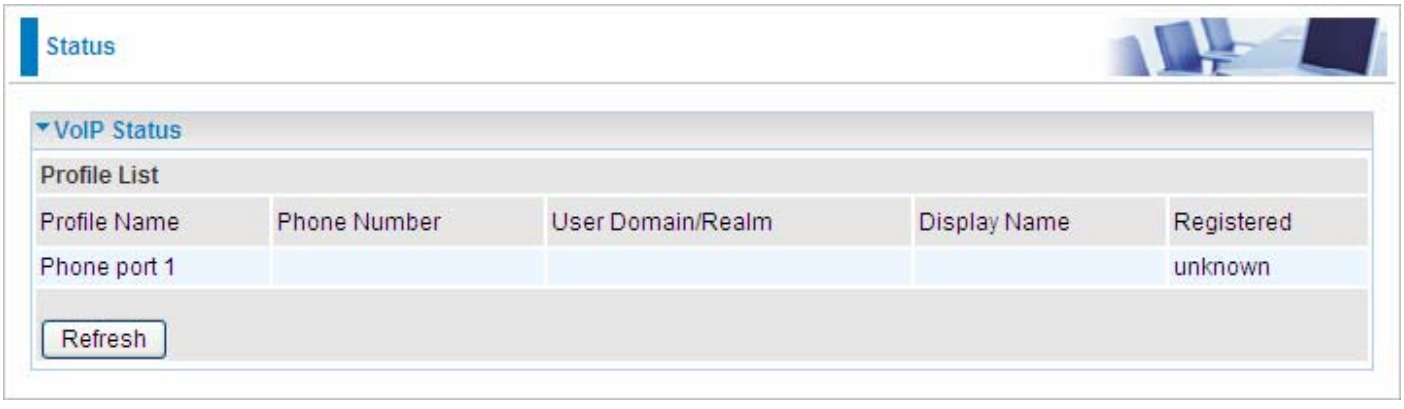


UPnP Portmap

This section lists all the established port-mapping using UPnP (Universal Plug and Play). See the Advanced section of this manual for more details on UPnP and the router UPnP configuration options.

VoIP Status

This table shows the status of the phone ports when VoIP feature has been activated. It displays information such as domain name, display name & phone number of the VoIP device.

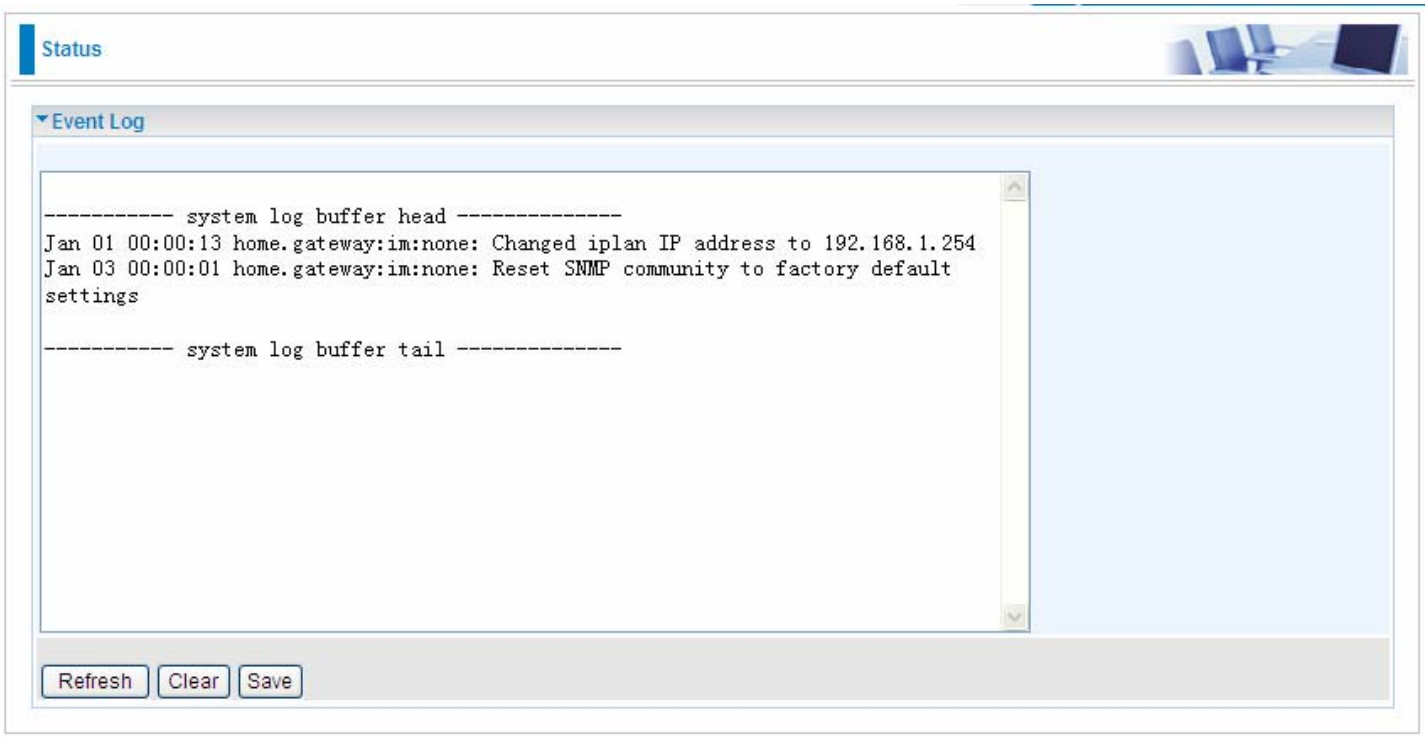


VoIP Call Log

The call log records the data from your VoIP devices such as the date / time of dial out calls, the duration of the calls, information about the missed calls and also incoming calls.

Event Log

This page displays all the event Log entries of the router such as when gets disconnected and during Firewall triggered events like Intrusion or Blocking Logging. Please see the Firewall section of this manual for more details on how to enable Firewall logging.


Status
Event Log
---------- system log buffer head ----------
Jan 01 00:00:13 home.gateway:im:none: Changed iplan IP address to 192.168.1.254
Jan 03 00:00:01 home.gateway:im:none: Reset SNMP community to factory default settings
---------- system log buffer tail ----------
Refresh
Clear
Save

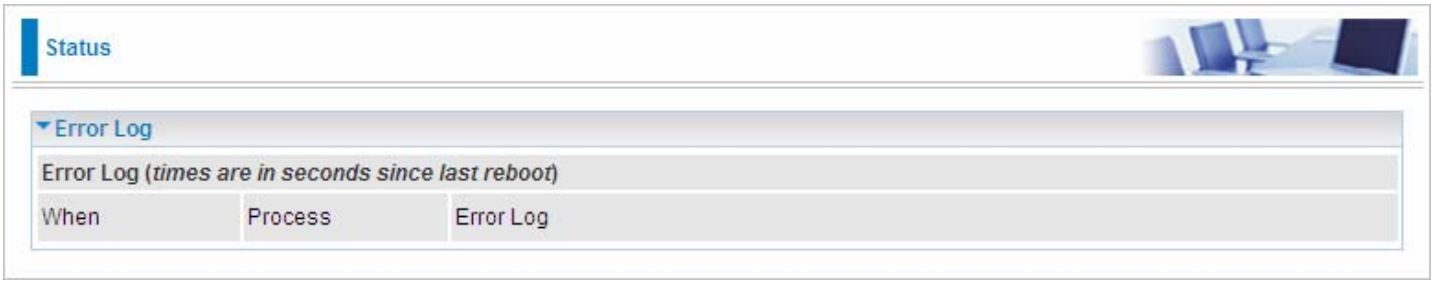
Click **Refresh** button to get the latest event log information.

Click **Clear** button to clear the log information.

Click **Save** button to backup the event log information to your computer. Click Save button, you will enter page as follows to save the backup to your computer.

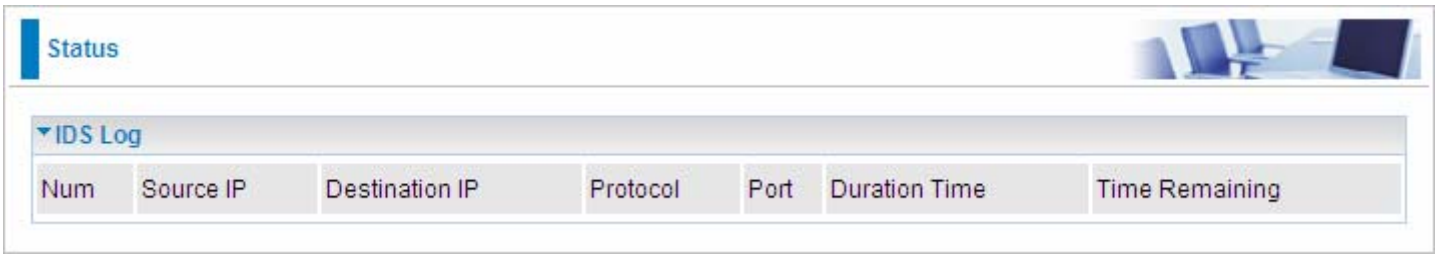
Error Log

Any errors encountered by the router (e.g. invalid names given to entries) are logged to this window.



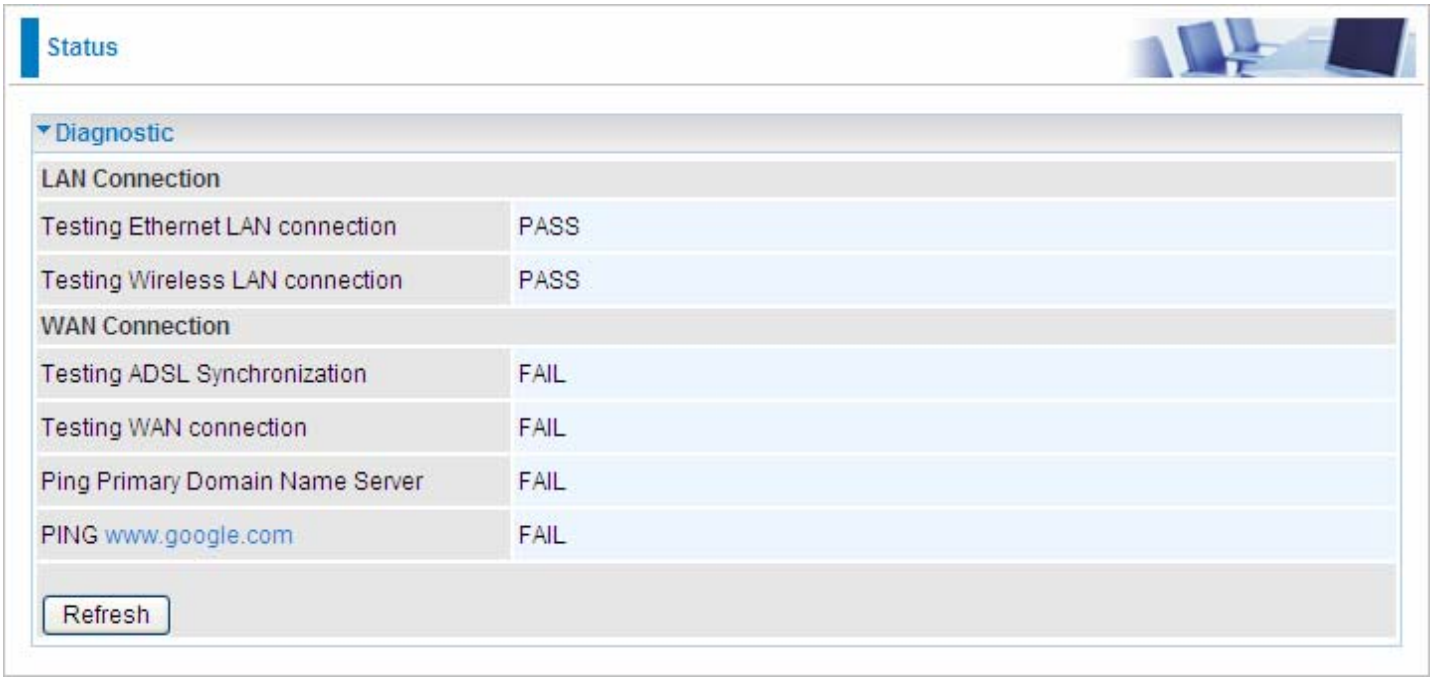
IDS Log

Any records about hacker attacks and intrusion attempts from the Internet are logged to this window.



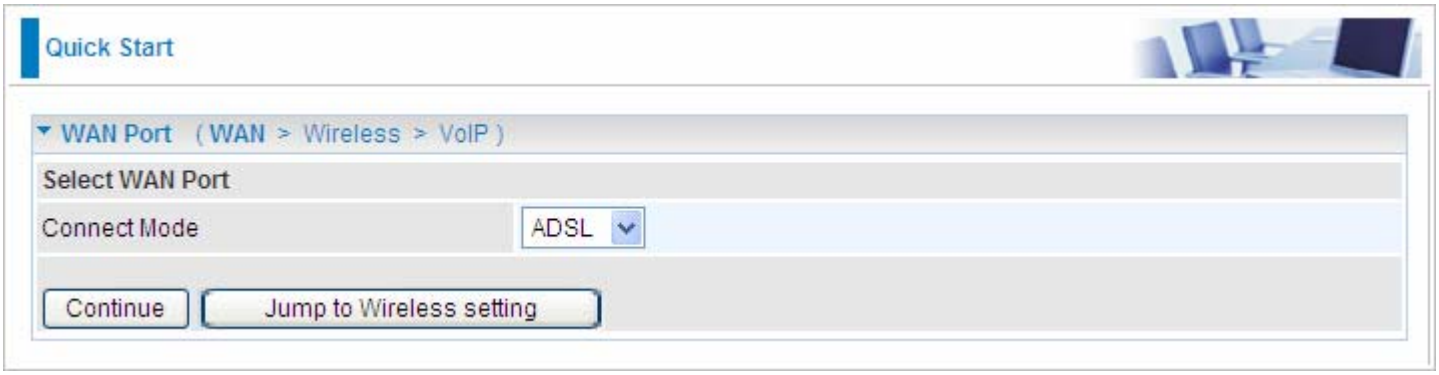
Diagnostic

It tests the connection to computer(s) which is connected to the LAN ports and also the WAN Internet connection. If PING **www.google.com** is shown FAIL and the rest is PASS, you ought to check your PC's DNS setting is correct.

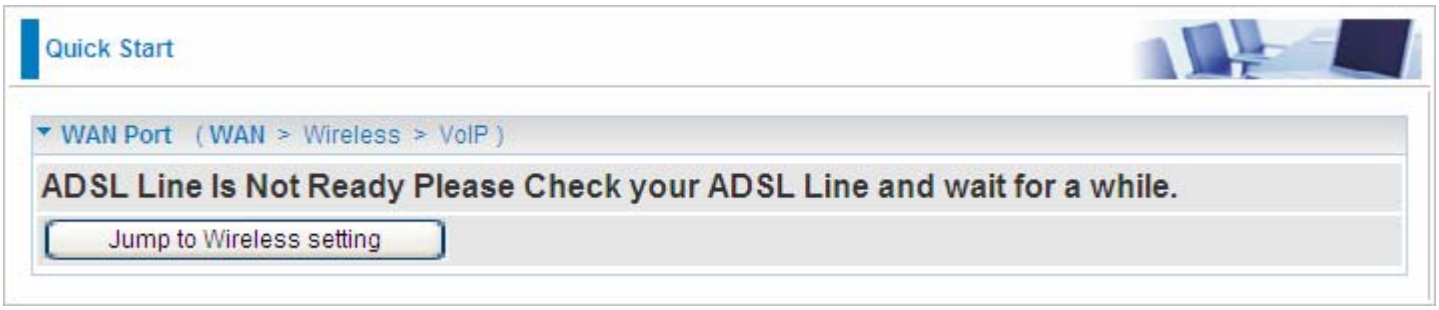


Quick Start

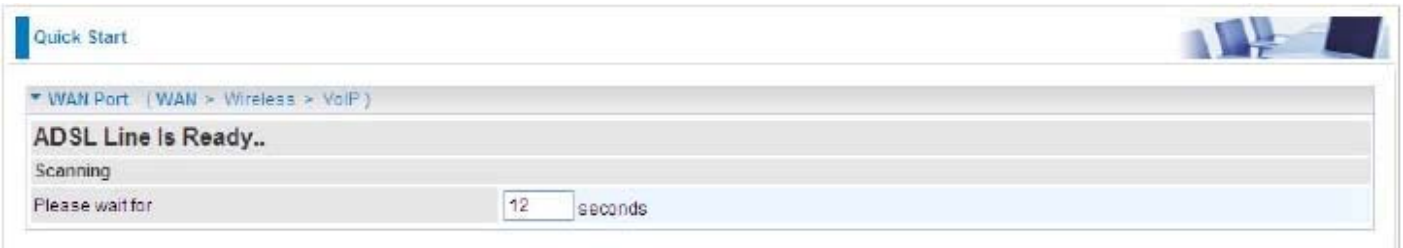
1. Click Quick Start. Select the connect mode you want. There are 2 options to choose from: ADSL or EWAN. Select ADSL mode from the drop down menu and click Continue.



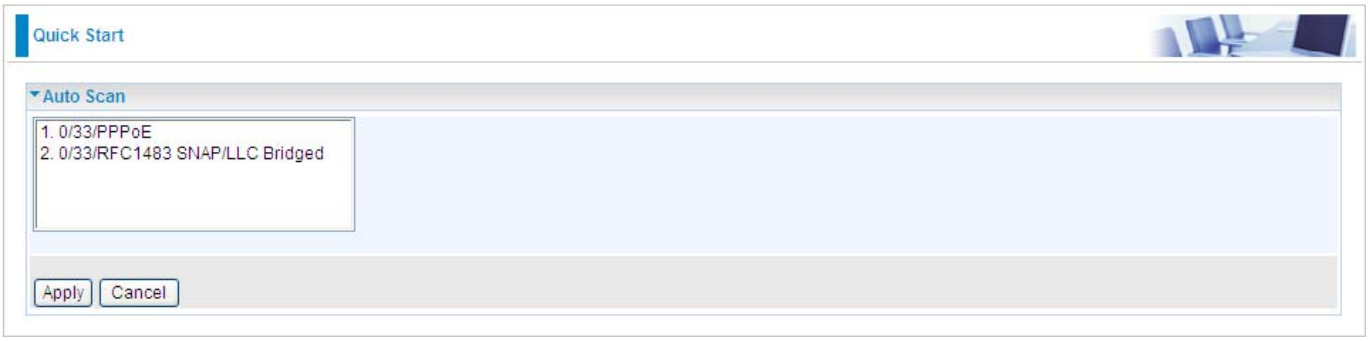
2. If your ADSL line is not ready, you need to check your ADSL line has been set or not.


Quick Start
WAN Port (WAN > Wireless > VoIP)
ADSL Line Is Not Ready Please Check your ADSL Line and wait for a while.
Jump to Wireless setting

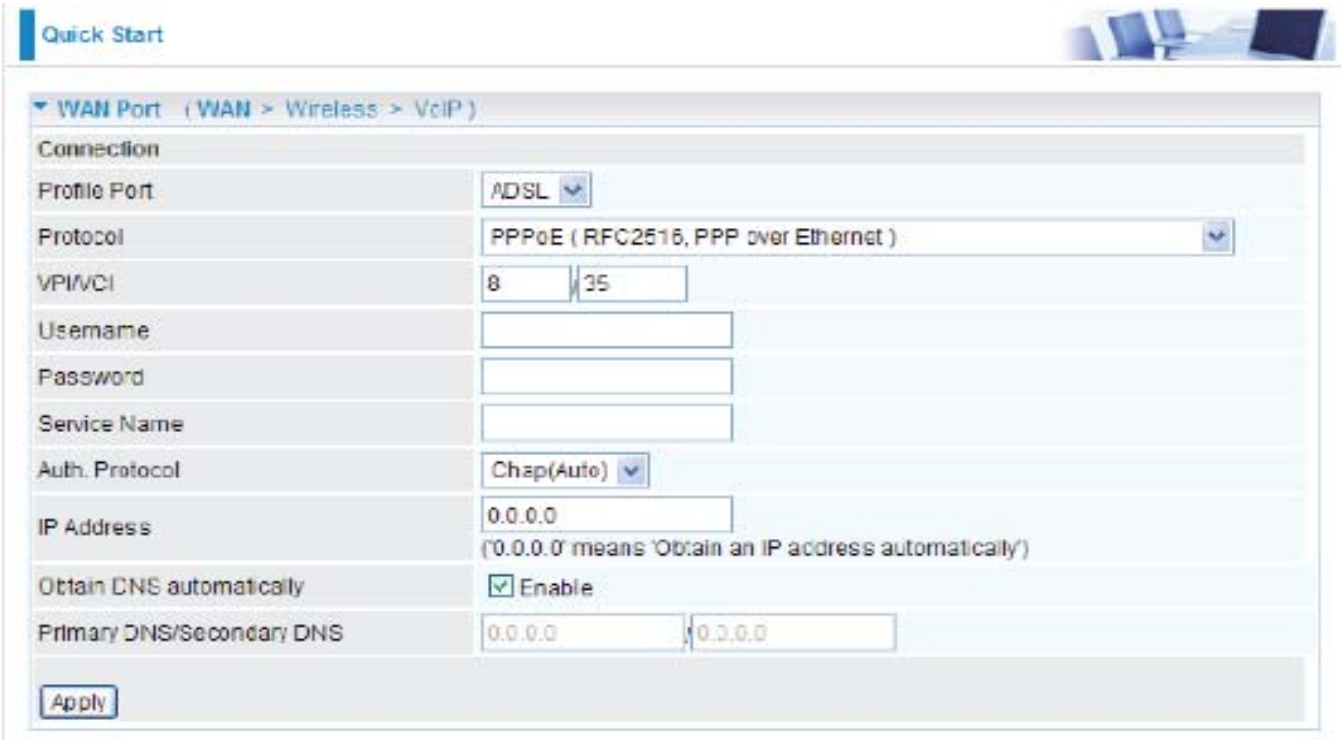
3. If your ADSL line is ready, the screen appears ADSL Line is Ready. Choose Auto radio button and click Apply. It will automatically scan the recommended mode for you. Manually mode makes you to set the ADSL line by manual. (If you choose Manually, you will directly go to step 5.)



4. The list below has different mode applied for your choice. Choose 0/33/PPPoE (Recommended) and click Apply.



5. Please enter “Username” and “Password” as supplied by your ISP (Internet Service Provider) and click Apply to continue.



Profile Port: Select the connection mode. There is ADSL**.**

Protocol: Select the protocol mode. The default mode is PPPoE.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

Service Name: This item is for identification purposes. If it is required, your ISP provides you the information.

Authentication Protocol: Default is **Auto.** Your ISP advises on using **Chap** or **Pap.**

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

Primary DNS / Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

6. Configure the Wireless LAN setting.

WLAN Service: Default setting is set to Enable. If you want to use wireless, both 802.11g and 802.11b device in your network, you can select Enable.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

ESSID Broadcast: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Enable.**

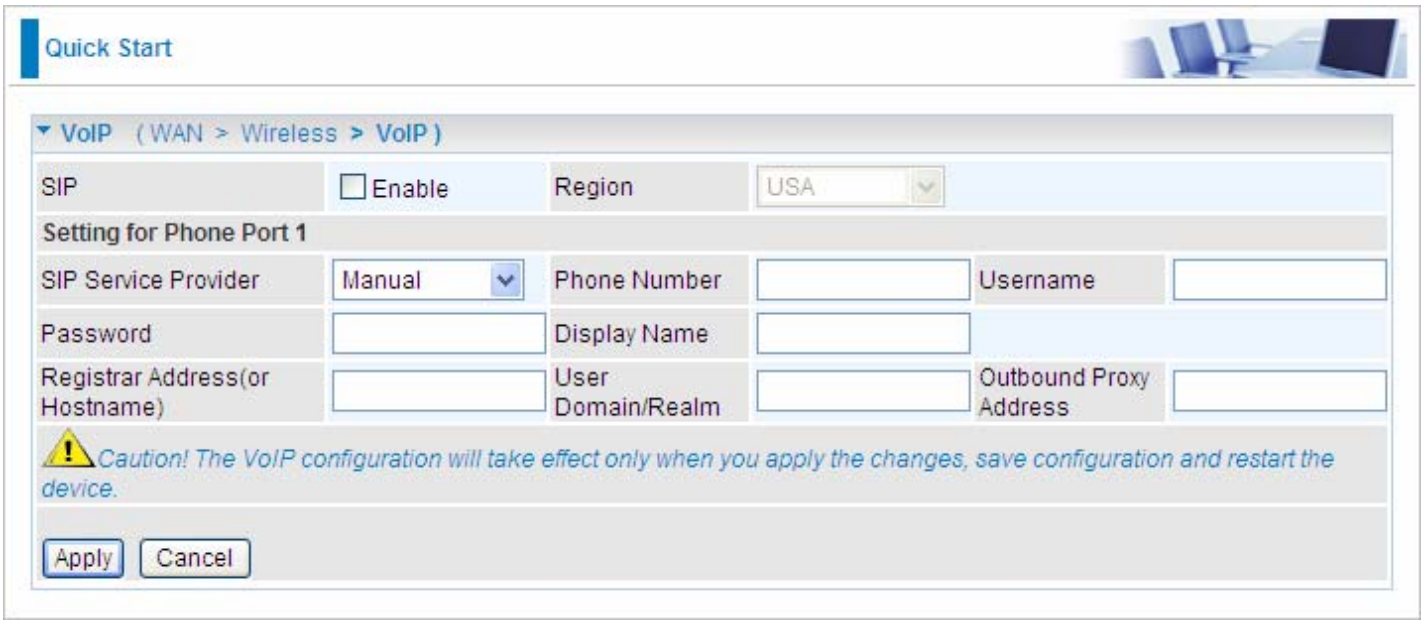
> **Enable:** When Enable is selected, you can allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.
>
> **Disable:** Select Disable if you do not want broadcast your ESSID. When select Disable, no one will be able to locate the Access Point (AP) of your router.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the ID channel that you would like to use.

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

7. Set up VoIP.



SIP: To use VoIP SIP as VoIP call signaling protocol. Default is set to ***Disable.***

Region: This selection is a drop-down box, which allows user to select the country for which the VoIP device must work. When a country is selected, the country parameters are automatically loaded.

SIP Service Provider: This section allows you to select the service provider. When the selection is done, respective parameters below are automatically displayed.

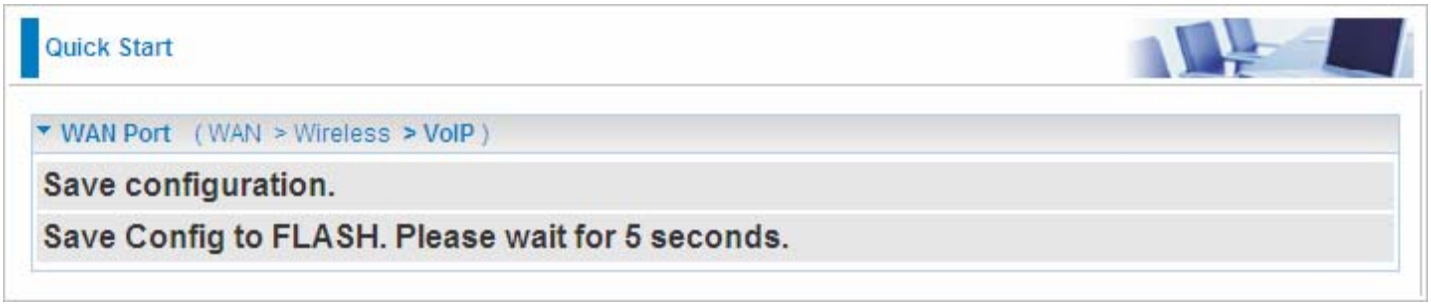
Phone Number: This parameter holds the registration ID of the user within the VoIP SIP registrar.

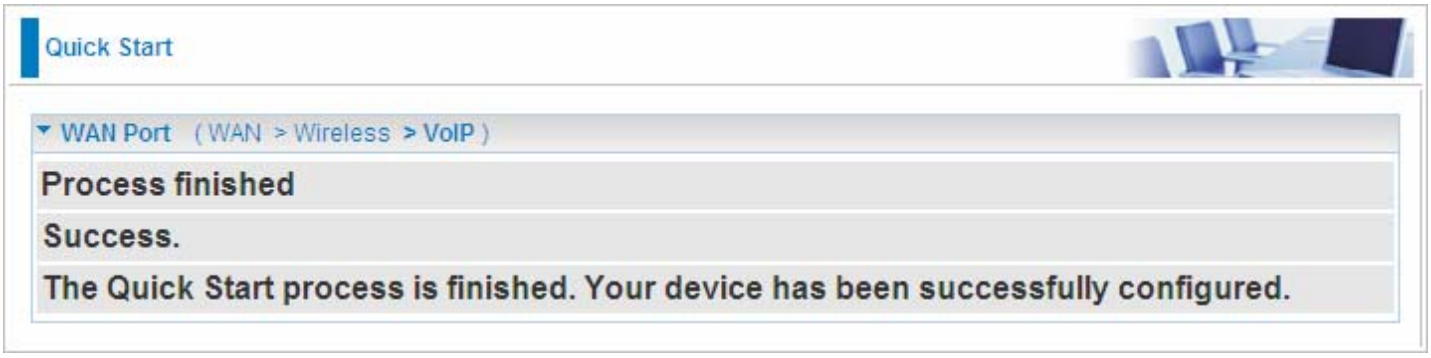
Username: If the username is same as the Phone Number, leave it blank. Otherwise, fill in the space with your username given by your VoIP provider.

Password: This parameter holds the password used for authentication within VoIP SIP registrar.

Display Name: This parameter will be appeared on the Caller ID.

8. Wait for the configuration.




Quick Start
WAN Port (WAN > Wireless > VoIP)
Process finished
Success.
The Quick Start process is finished. Your device has been successfully configured.

9. When ADSL is synchronic, it will appear “check”.

Configuration

When you click this item, the column will expand to display the sub-items that will allow you to further configure your router.

LAN, WAN, System, Firewall, VoIP, QoS, Virtual Server, Wake on LAN, Time Schedule and Advanced

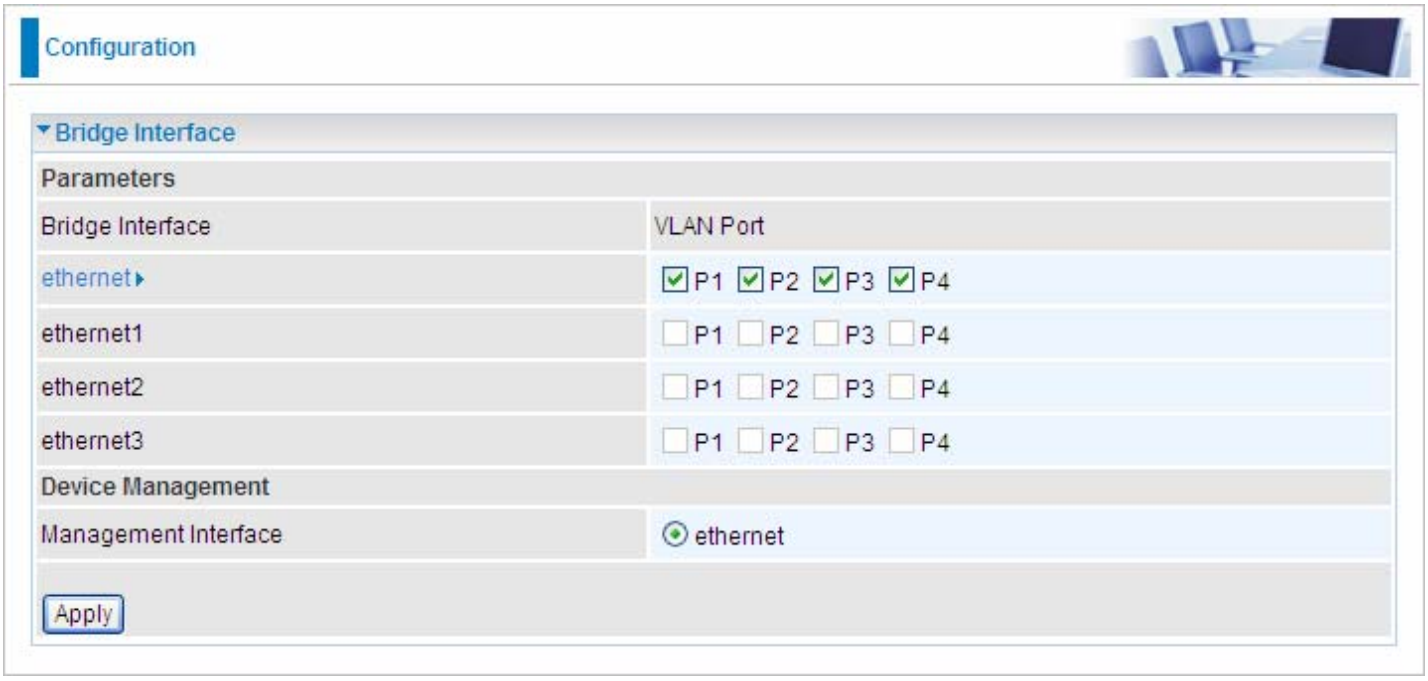
The function of each configuration sub-item is described in the following sections.

LAN - Local Area Network

Here are the items within the LAN section: **Bridge Interface, Ethernet, IP Alias, IPv6 Autoconfig, Ethernet Client Filter, Wireless, Wireless Security, Wireless Client Filter, WPS, Port Setting** and **DHCP Server.**

Bridge Interface

You can setup member ports for each VLAN group under Bridge Interface section.



Ethernet: P1 & P2 (Port 1, 2)

Ethernet1: P3, P4 & Wireless (Port 3, 4 & wireless). Uncheck P3, P4 & Wireless from Ethernet VLAN port first.

Note: You should setup each VLAN group with caution. Each Bridge Interface is arranged in this order.

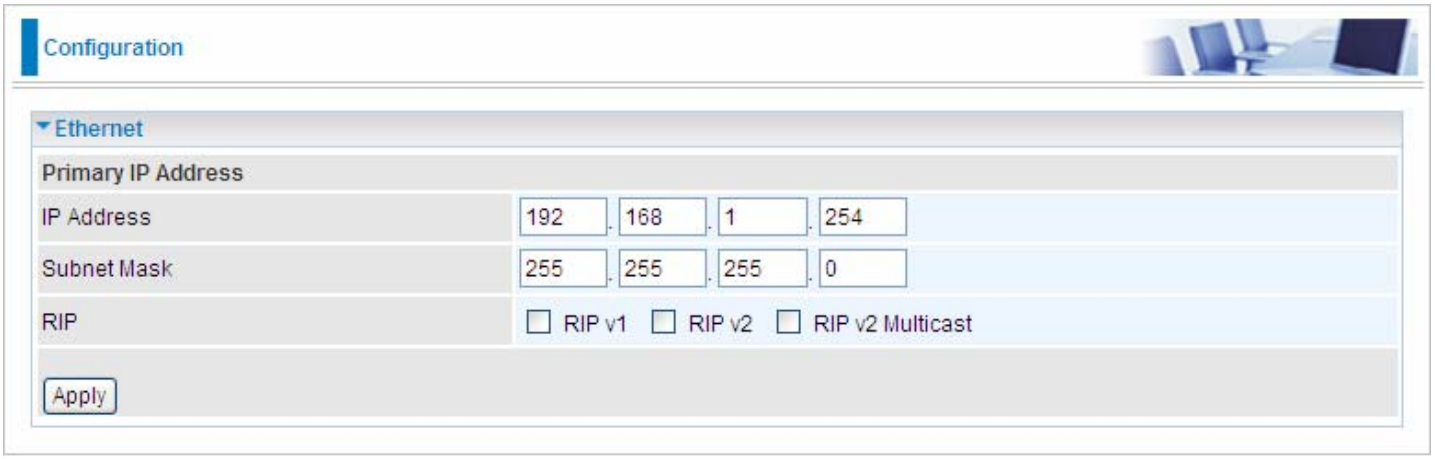
Bridge Interface	VLAN Port (Always starts with)
ethernet	P1 / P2 / P3 / P4 / Wireless
ethernet1	P2 / P3 / P4 / Wireless
ethernet2	P3 / P4 / Wireless
ethernet3	P4 / Wireless
Wireless	Wireless

Management Interface: To specify which VLAN group is possible to perform device management, like doing web management.

Note: NAT/NAPT can be applied to management interface only.

Ethernet

The router supports more than one Ethernet IP addresses in the LAN that supports multiple internet access at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.



Primary IP Address

IP Address: The default IP on this router.

Subnet Mask: The default subnet mask on this router.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

IP Alias

This function enables the creation of multiple virtual IP interfaces for this router. It helps to connect two or more local networks to the ISP or remote node. In this case, an internal router is not required.

IP Address: Specify an IP address for this virtual interface.

Netmask: Specify a subnet mask for this virtual interface.

Security Interface: Specify the firewall setting for this virtual interface.

Internal: This mean the network is behind NAT. All traffic will do network address translation when sending out data to the Internet if NAT is enabled.

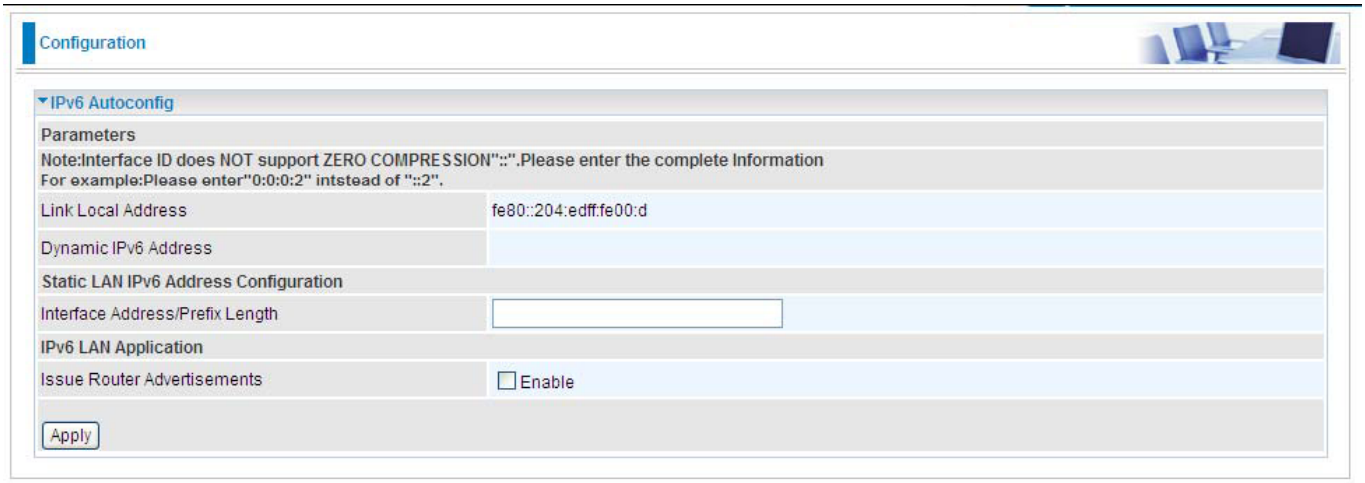
External: This means there is no NAT on this IP interface and it is connected directly to the Internet. This function is mostly used when you are provided with multiple public IP addresses by the ISP. In this case, you can use the public IP address in the local network whose gateway IP address points to the IP address on this interface.

DMZ: Specify this network to a DMZ area. There is no NAT on this interface.

IPv6 Autoconfig

The IPv6 address composes of two parts, thus, the prefix and the interface ID.

BiPAC 7401VGP R3 dynamically configure IPv6 address on host with Stateless auto-configuration mode. Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information(prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn't configure anything on the client.



Link Local Address: the Link local address for this device.

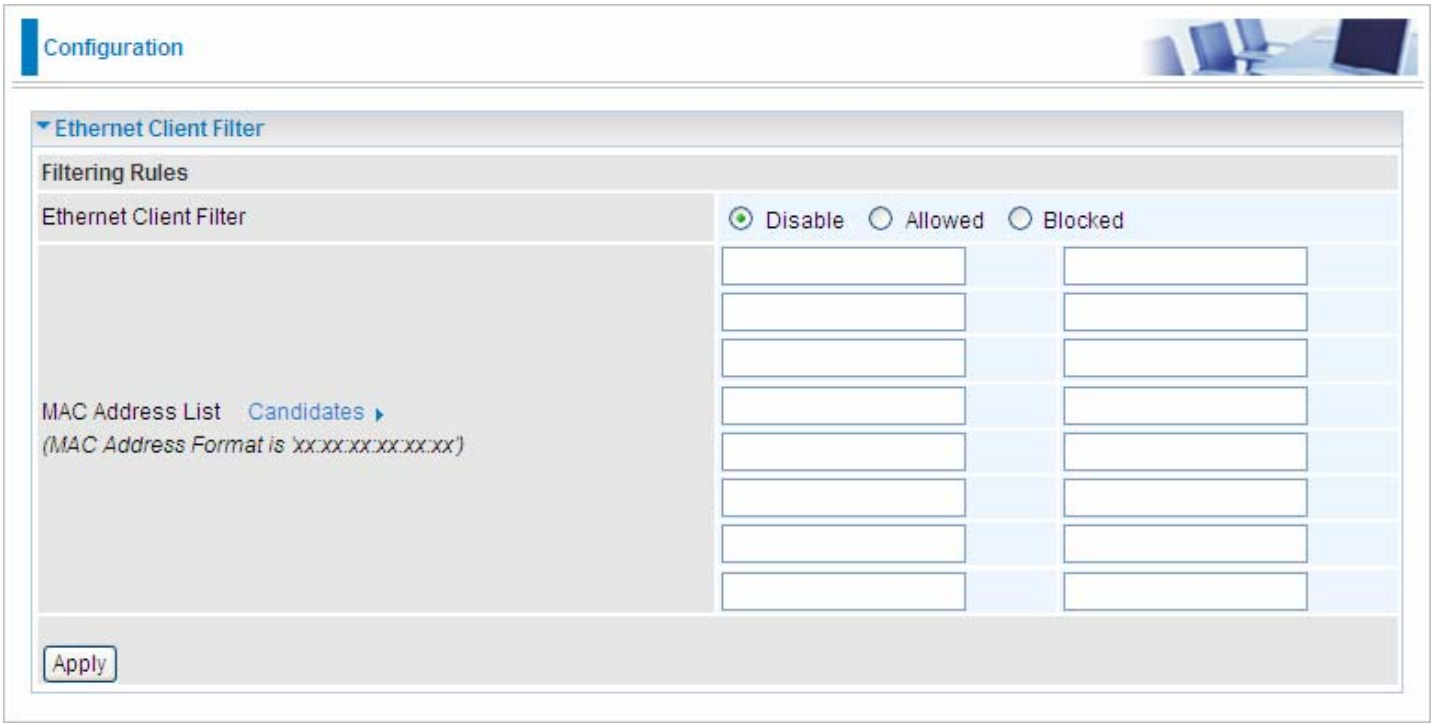
Dynamic IPv6 Address: this field displays the dynamic obtained IPv6 address if you haven't set static IPv6 address.

Interface Address/Prefix length: enter the static LAN IPv6 address.

Issue Router Advertisements: check whether to enable issue Router Advertisement feature. It is to send Router Advertisement messages periodically.

Ethernet Client Filter

The Ethernet Client Filter can support up to 16 Ethernet network computers. It enables you to accept traffic from specific authorized computers or can restrict unwanted computer(s) to access your LAN.
There are no pre-defined Ethernet MAC address filter rules, you can add the filter rules to meet your requirements.



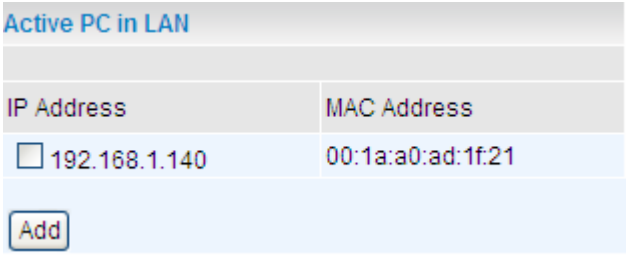
Ethernet Client Filter: Default setting is set **Disable**.

Allowed: check to enable a specific PC to access your LAN by inserting the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is listed.

Blocked: check to prevent an unwanted PC from accessing your LAN by inserting the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is not listed.

The maximum number of client is 16. The MAC addresses should be 6 bytes long and are presented only in hexadecimal characters. Only numbers (0 - 9) and letters (a - f) are acceptable.

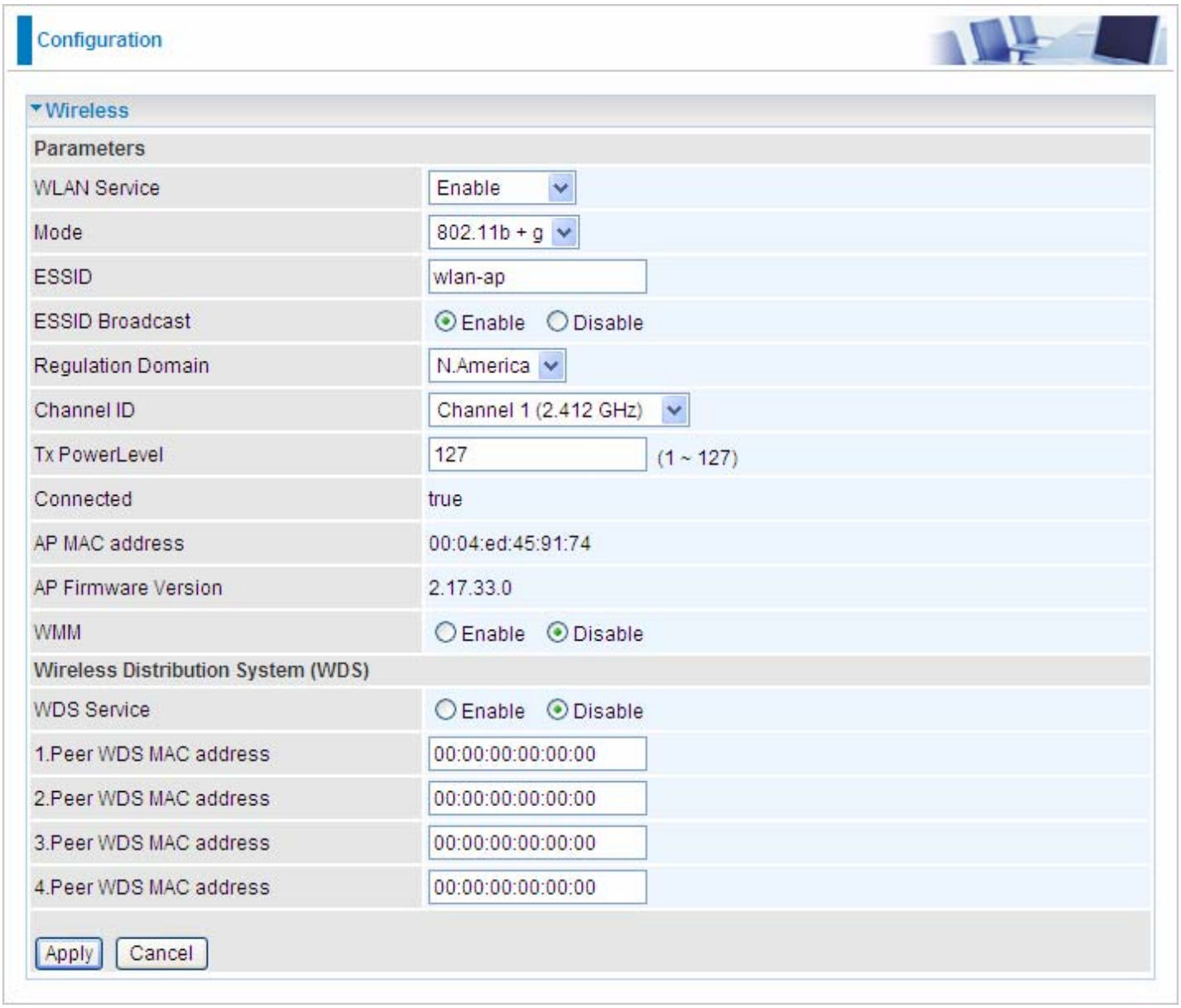
Note: Follow the MAC Address Format xx:xx:xx:xx:xx:xx. Semicolon (:) must be included.
Candidates: automatically detects devices that are connected to the router through the Ethernet. Click the Candidate button to access the **Active PC in LAN** window.



Active PC in LAN: Active PC in LAN window displays a list of IP Address & MAC Address of each Ethernet device which connects to the router.
You can check the checkbox next to the IP address to block or to allow the PC from accessing the

LAN. Then, click Add to insert the IP to the Ethernet Client Filter table. The maximum number of supported Ethernet client is 16.

Wireless



Parameters

WLAN Service: Choose Disabled/Enable/TimeSlot from the drop-down list.

Mode: The default setting is 802.11b+g (Mixed mode). If you do not know or do not have both 11g and 11b devices on your network, then keep the setting in mixed mode. From the drop-down menu, you can select 802.11g if you have only 11g card. If you have only 11b card, then select 802.11b.

ESSID: The ESSID is a unique name of a wireless access point (AP) used to distinguish one from another. For security purpose, change the default wlan-ap to a unique ID name that is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Note: It is case sensitive and must not exceed 32 characters.

ESSID Broadcast: It is used to broadcast its ESSID on the network so that when a wireless client searches for a network, the router can be discovered and recognized. Default setting is **Enable.**

Enable: When enabled, you allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.

Disable: When disabled, you do not broadcast your ESSID. Therefore, no one will be able to locate the Access Point (AP) of your router.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection ID channel that you would like to use.
Note: Wireless performance may degrade if the selected ID channel is already being occupied by other AP(s).

TX PowerLevel: It is a function that enhances the wireless transmission signal strength. User may adjust this power level from minimum 1 up to maximum 100 or 127 depending on the models used. Please refer to the note table for the appropriate power level range of your model.

Note: The Power Level maybe different in each access network user premises environment so choose the most suitable level for your network.

Connected: Display either as true or false. That it is the connection status between the system and the build-in wireless card.

AP MAC Address: It is a unique hardware address of the Access Point.

AP Firmware Version: The Access Point firmware version.

WMM: This feature works concurrently with QoS that enables the system to prioritize the flow of data packets according to 4 categories: Voice, Video, Best Efforts and Background.

Enable: Click to activate WMM feature.

Disable: Click to deactivate WMM feature.

Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access points. It is easy to install simply by defining the peer's MAC address of the connected AP. WDS takes advantage of the cost saving and flexibility with no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network. It can connect up to 4 wireless APs for extending cover range at the same time.

In addition, WDS also enhances its link connection security mode. Key encryption and channel must be the same for both access points.

WDS Service: The default setting is **Disabled.** Check **Enable** radio button to activate this function.

1. **Peer WDS MAC Address:** It is the associated AP MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.

2. **Peer WDS MAC Address:** It is the second associated AP MAC Address.

3. **Peer WDS MAC Address:** It is the third associated AP MAC Address.

4. **Peer WDS MAC Address:** It is the fourth associated AP MAC Address.

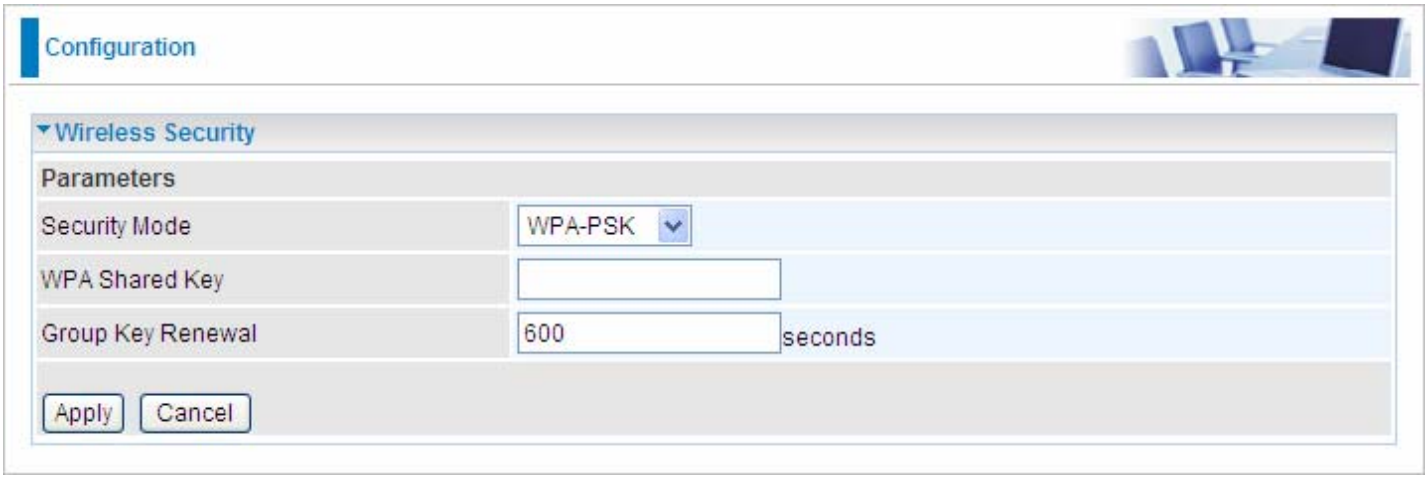
Note: For MAC Address, Semicolon (:) must be included.

Wireless Security

You can disable or enable the wireless security function using WPA or WEP for wireless network protection.

The default mode of wireless security is set to disabled.

WPA-PSK / WPA2-PSK

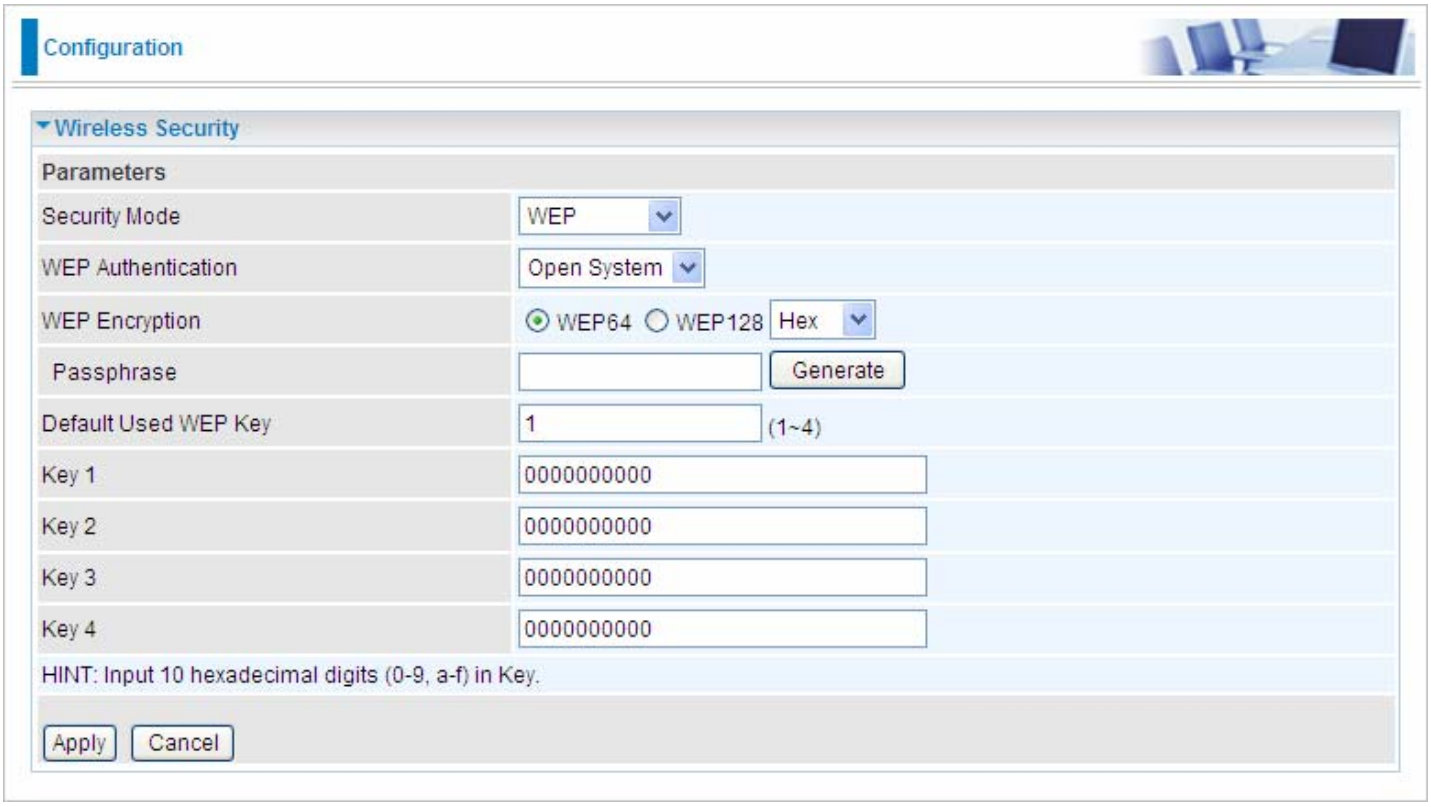


Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is **600** seconds.

WEP



WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are two options to select from: **Open System, Share key**.

WEP Encryption: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP. If you require high security for transmissions, there are two alternatives to select from: **WEP 64 and WEP 128**. WEP 128 will offer increased security over WEP 64.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

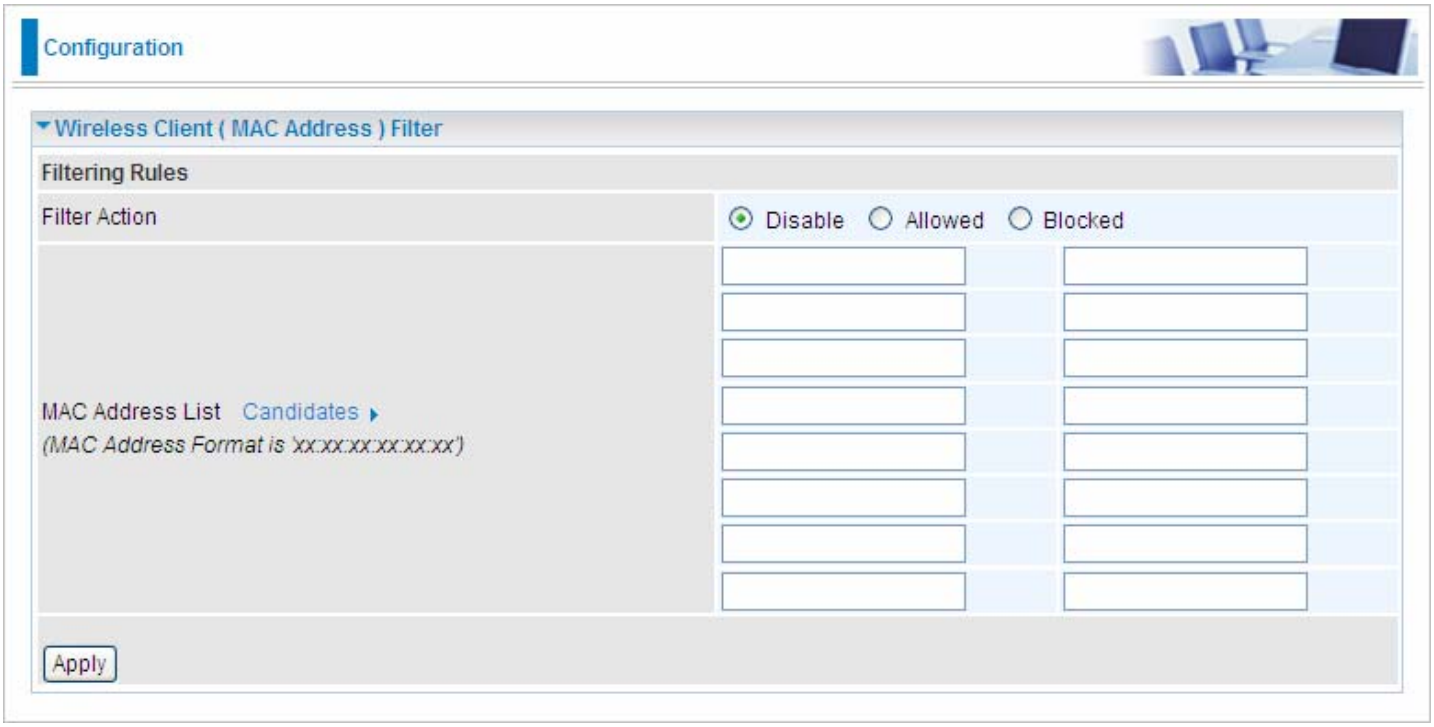
Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 10 and 26 HEX codes are required for WEP64 and WEP128 respectively.

Wireless Client / MAC Address Filter

The MAC Address supports up to 16 wireless network PCs and helps you manage your network control to accept traffic from specific authorized PCs or to restrict unwanted PC(s) to access your LAN.

There are no pre-defined MAC Address filter rules; you can add the filter rules to meet your requirements。



Filter Action: Default setting is set to **Disable**.

Allowed: To authorize specific device to access your LAN by insert the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is listed.

Blocked: To prevent unwanted device from accessing the LAN by insert the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is not listed.

The maximum client is 16. The MAC addresses are 6 bytes long; they are presented only in hexadecimal characters. The number **0** - **9** and letters **a** - **f** are acceptable.

Note: Follow the MAC Address Format xx:xx:xx:xx:xx:xx. Semicolon (:) must be included.

Candidates: It automatically detects for devices that are connected to the router through the Wireless feature.

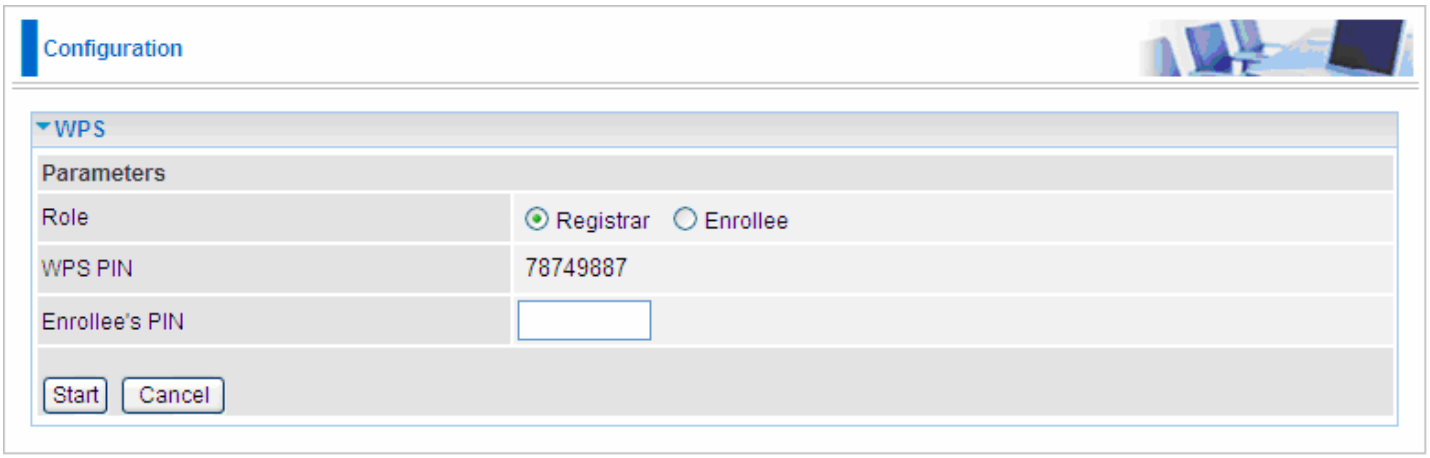
Click the Candidate button to access the **Associated Wireless Client** window.

Associate Wireless Client: Displays a list MAC addresses of all wireless devices that are currently connected to the router.

You can check the checkbox next to the MAC address to block or allow the wireless client to access the network. Then, Add to insert to the Wireless Client (MAC Address) Filter table. The maximum Wireless client is 16.

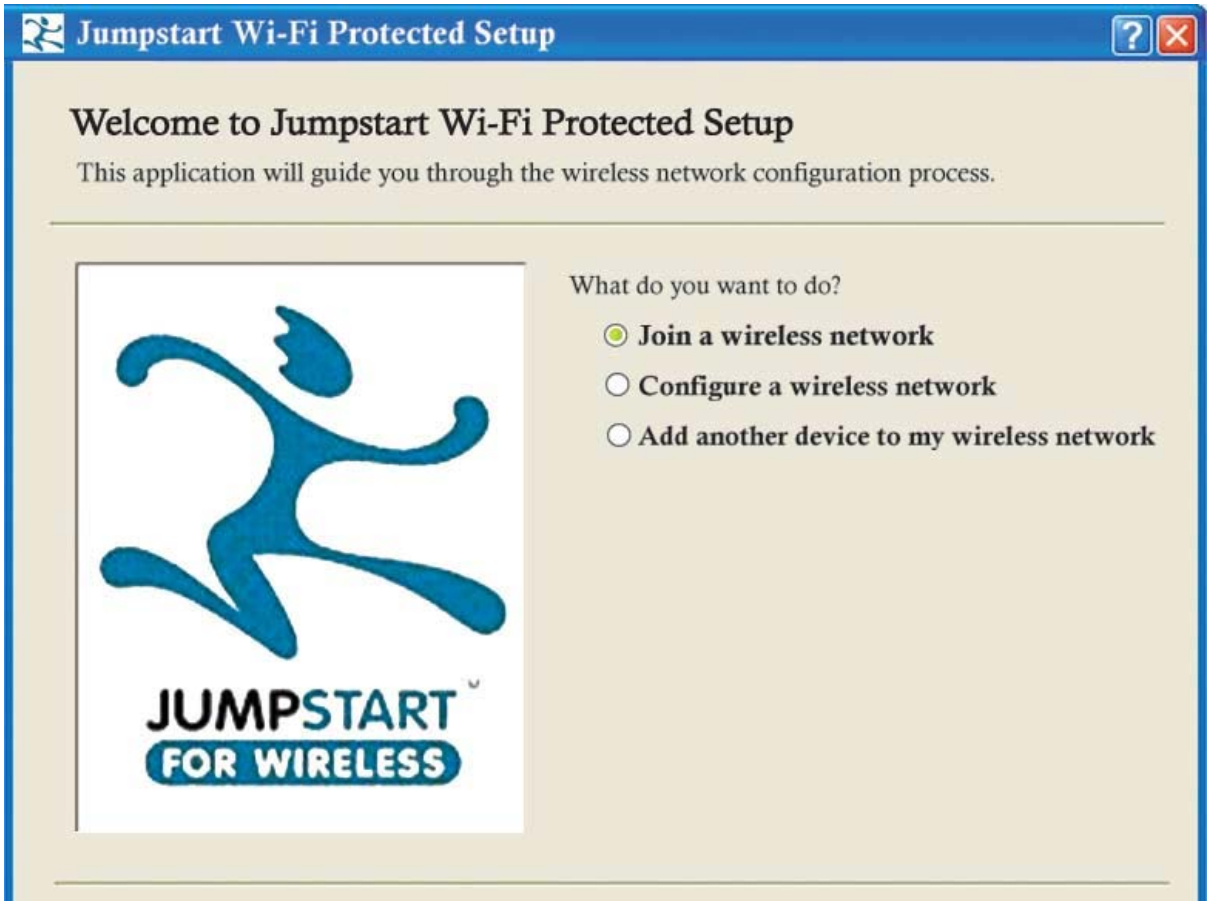
WPS

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This protocol is used to build a Wi-Fi network within a home / small office environment in an easy and secured manner. This feature thus provides a much simplified method to configure Wi-Fi Protected Access to those who know very little about wireless security.

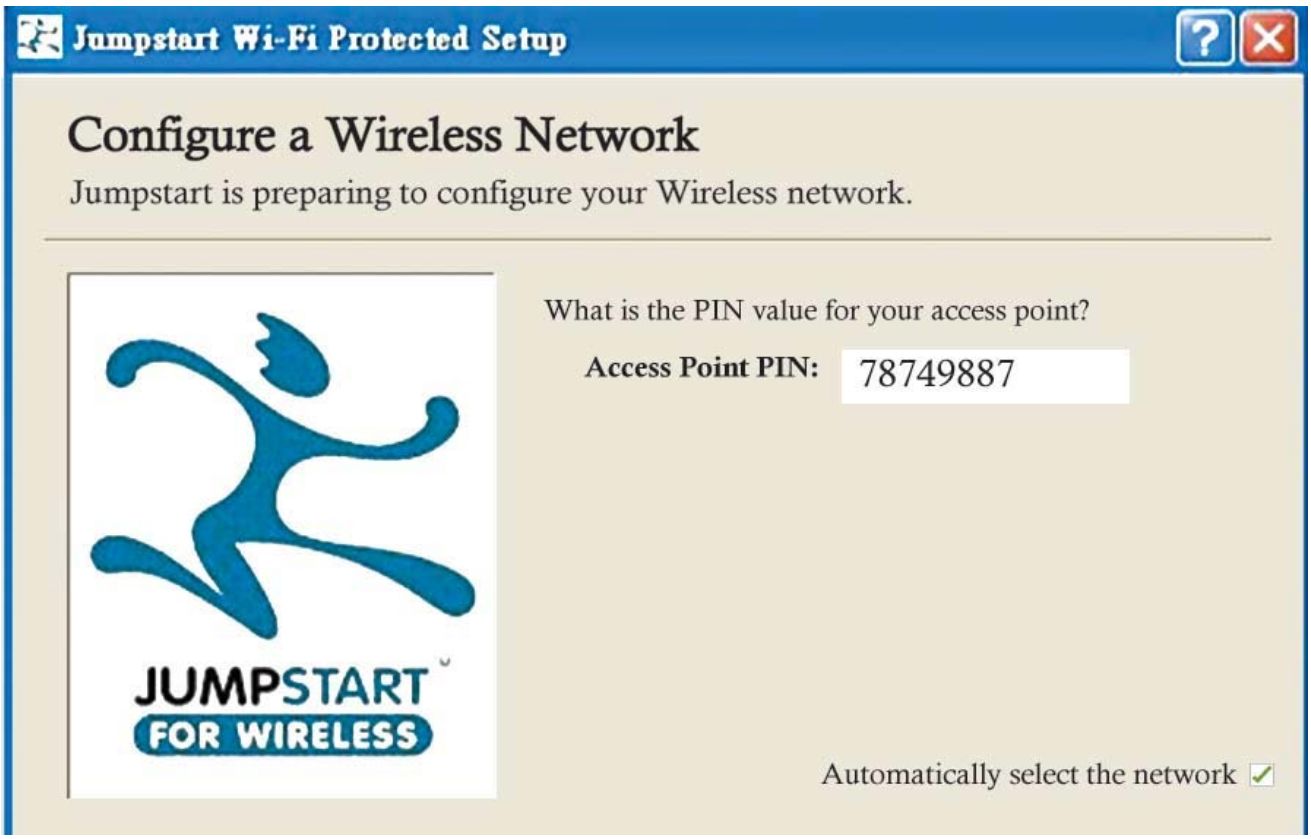


Security-enabled WiFi Network Setup

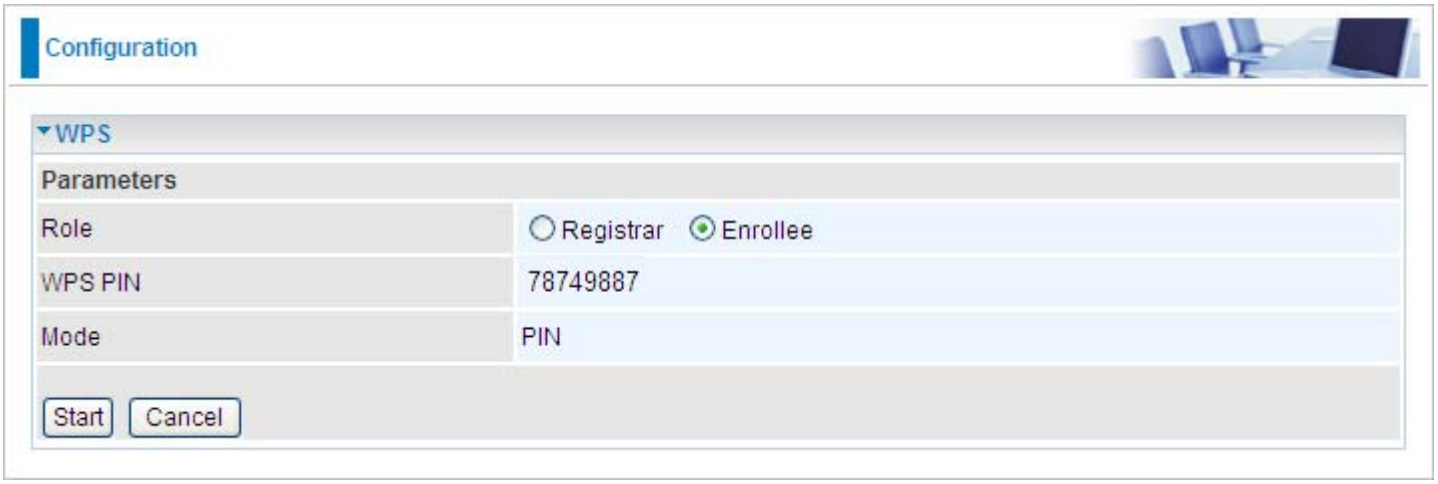
1. Jot down the AP Pin from the Web (eg. 78749887).
2. Launch the wireless client WPS utility (Ex: Atheros Jumpstart WPS utility), select “Configure a wireless network” and apply “next” button.


Jumpstart Wi-Fi Protected Setup
Welcome to Jumpstart Wi-Fi Protected Setup
This application will guide you through the wireless network configuration process.
What do you want to do?
Join a wireless network
Configure a wireless network
Add another device to my wireless network
JUMPSTART
FOR WIRELESS

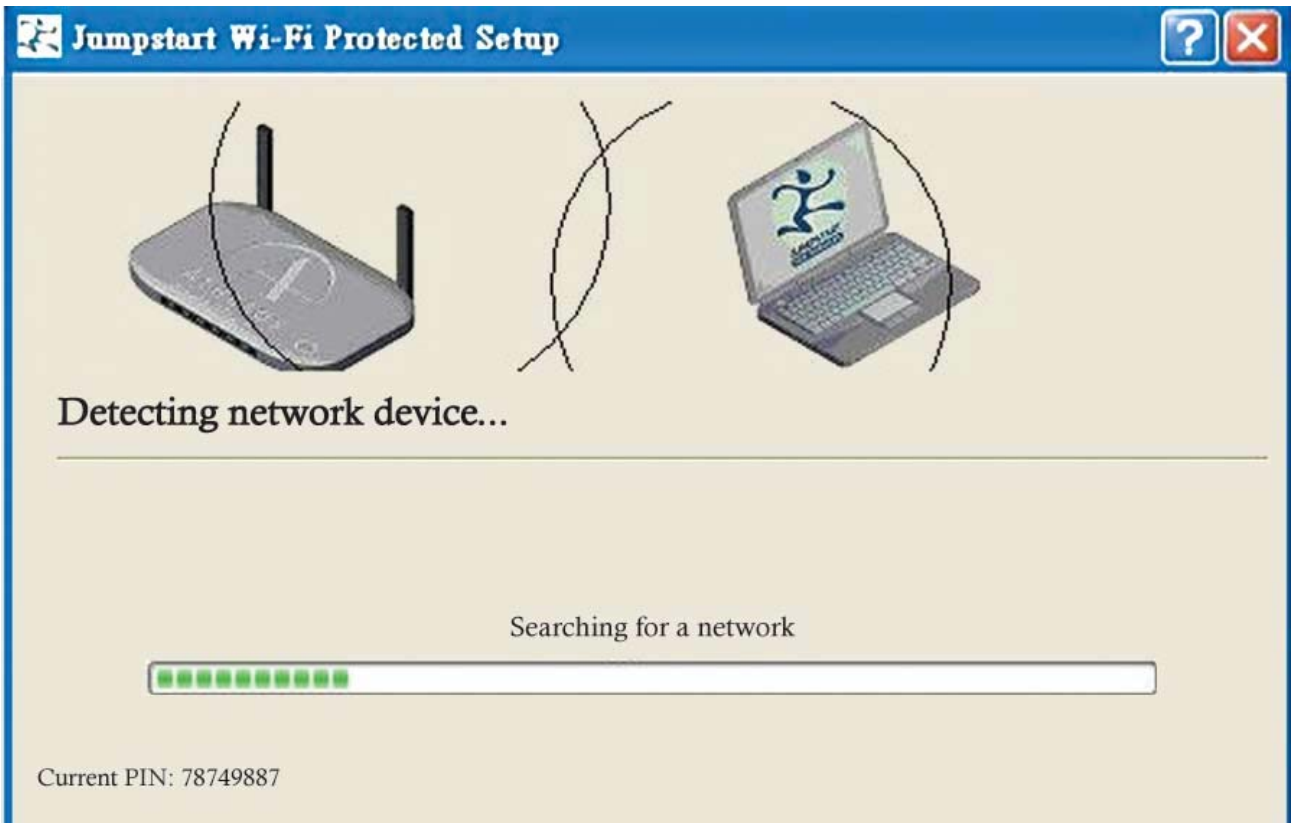
3. Enter the AP PIN into the utility and click on the “next” button.


Jumpstart Wi-Fi Protected Setup
Configure a Wireless Network
Jumpstart is preparing to configure your Wireless network.
JUMPSTART
FOR WIRELESS
What is the PIN value for your access point?
Access Point PIN:
78749887
Automatically select the network

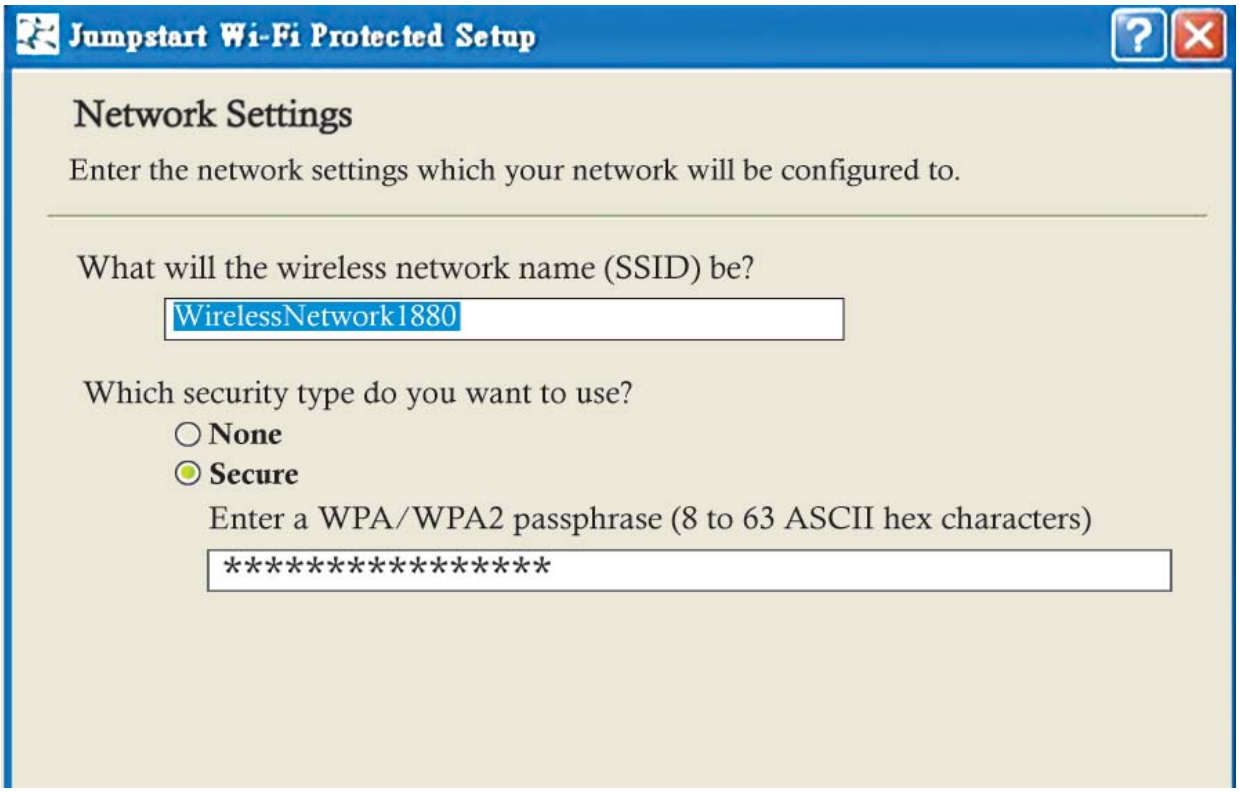
4. There are 2 ways to trigger the AP as Enrollee:
   Push the AP WPS button for 1 second and release it. Or In the WPS configuration page, click on the Enrollee radio button and then click the Start button.



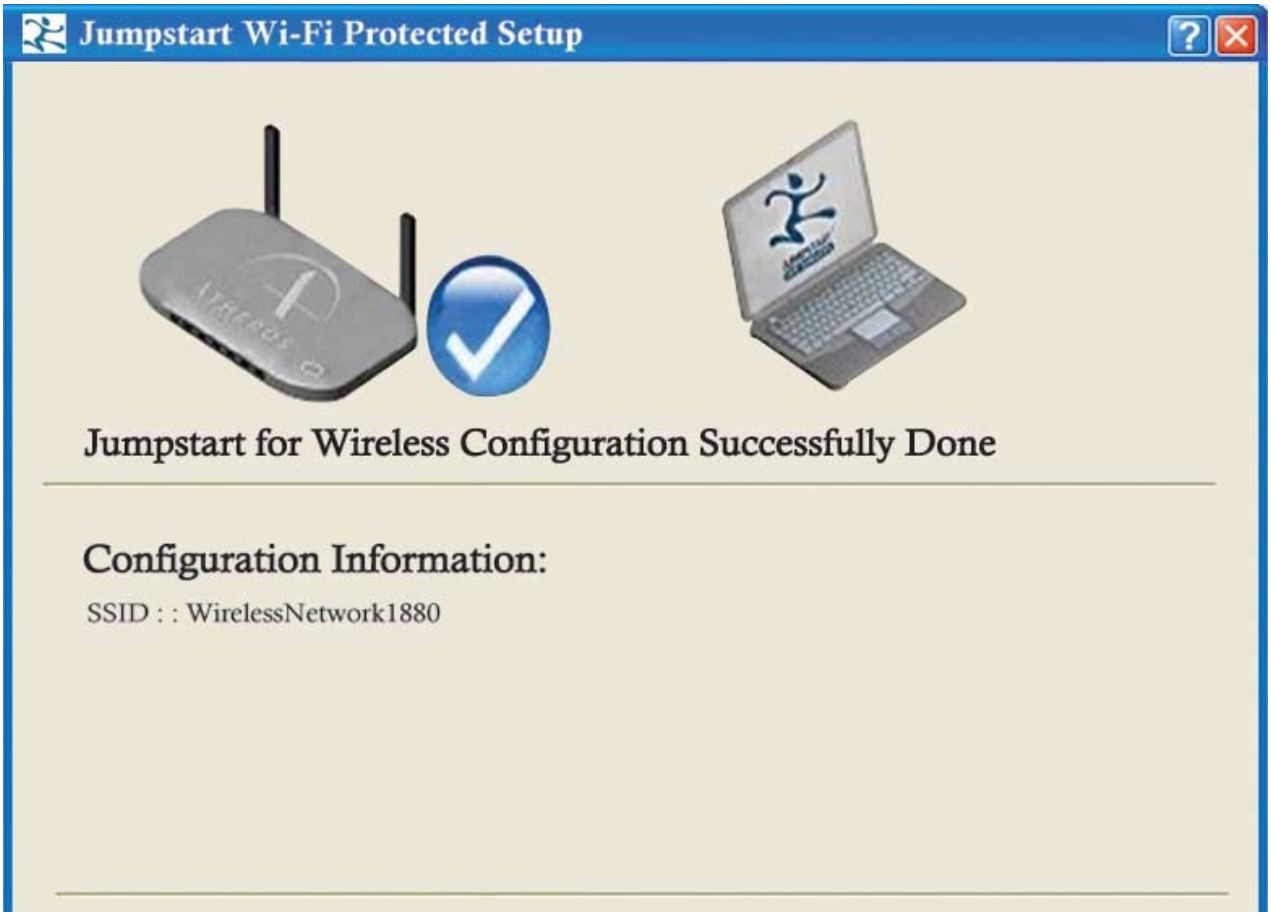
5. The utility will then search for the WPS AP.



6. SSID and security will be generated automatically (You may change it) and then press the Next button.


Jumpstart Wi-Fi Protected Setup
Network Settings
Enter the network settings which your network will be configured to.
What will the wireless network name (SSID) be?
WirelessNetwork1880
Which security type do you want to use?
None
Secure
Enter a WPA/WPA2 passphrase (8 to 63 ASCII hex characters)
****

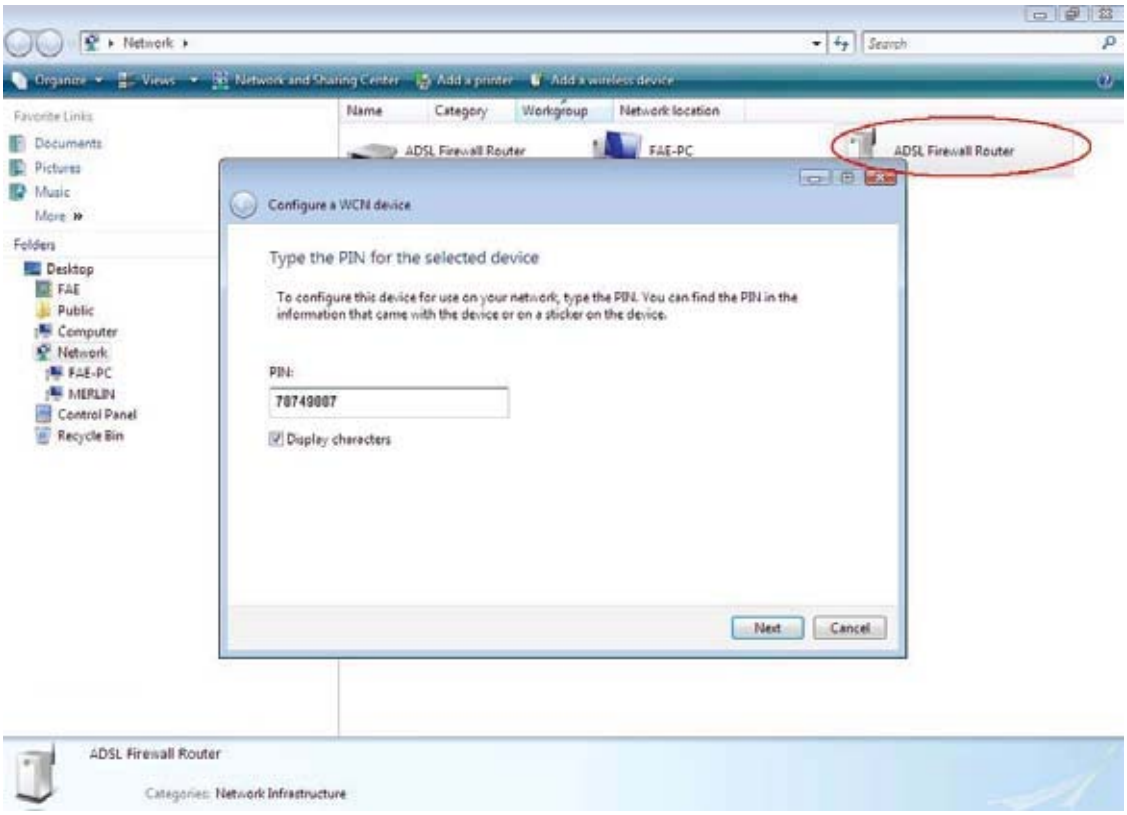
7. Your WPS setup is now complete and you will now have security enabled WiFi network.


Jumpstart Wi-Fi Protected Setup
Jumpstart for Wireless Configuration Successfully Done
Configuration Information:
SSID : : WirelessNetwork1880

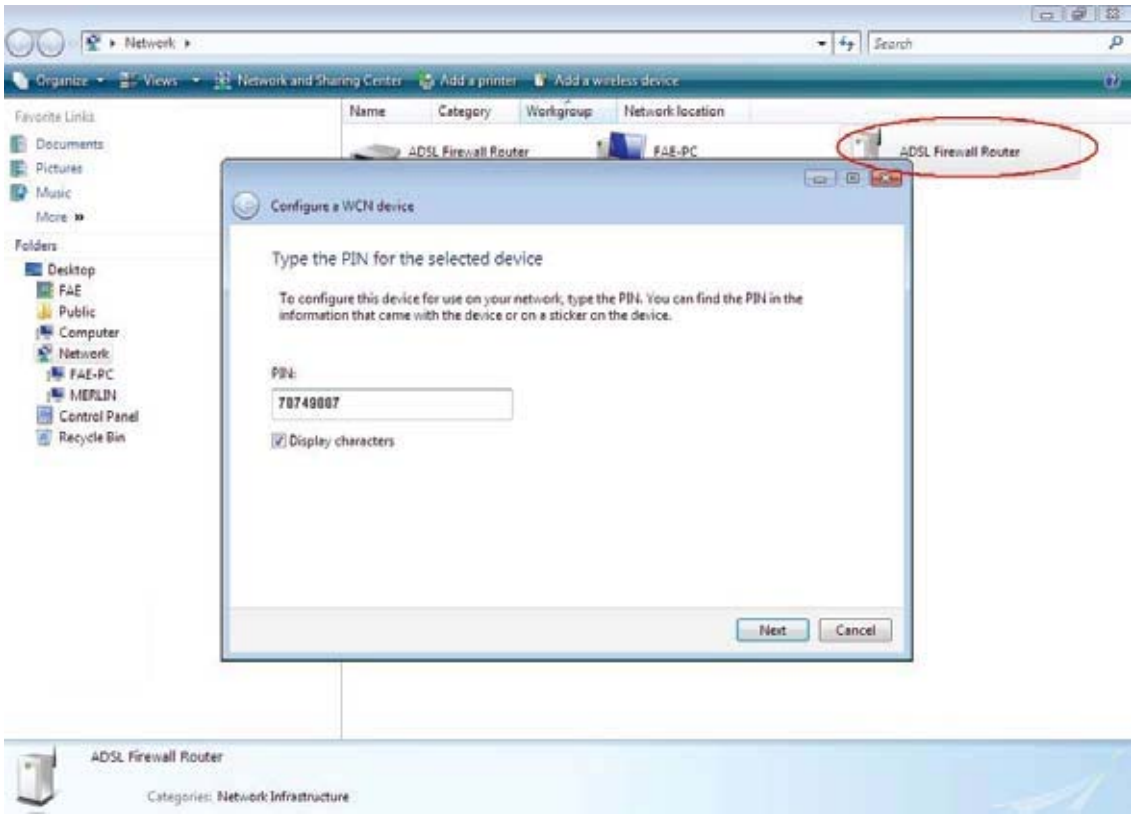
Setup Security-enabled Wi-Fi network using WCN in Vista

1. Jot down the AP PIN from the Web (eg. 78749887).

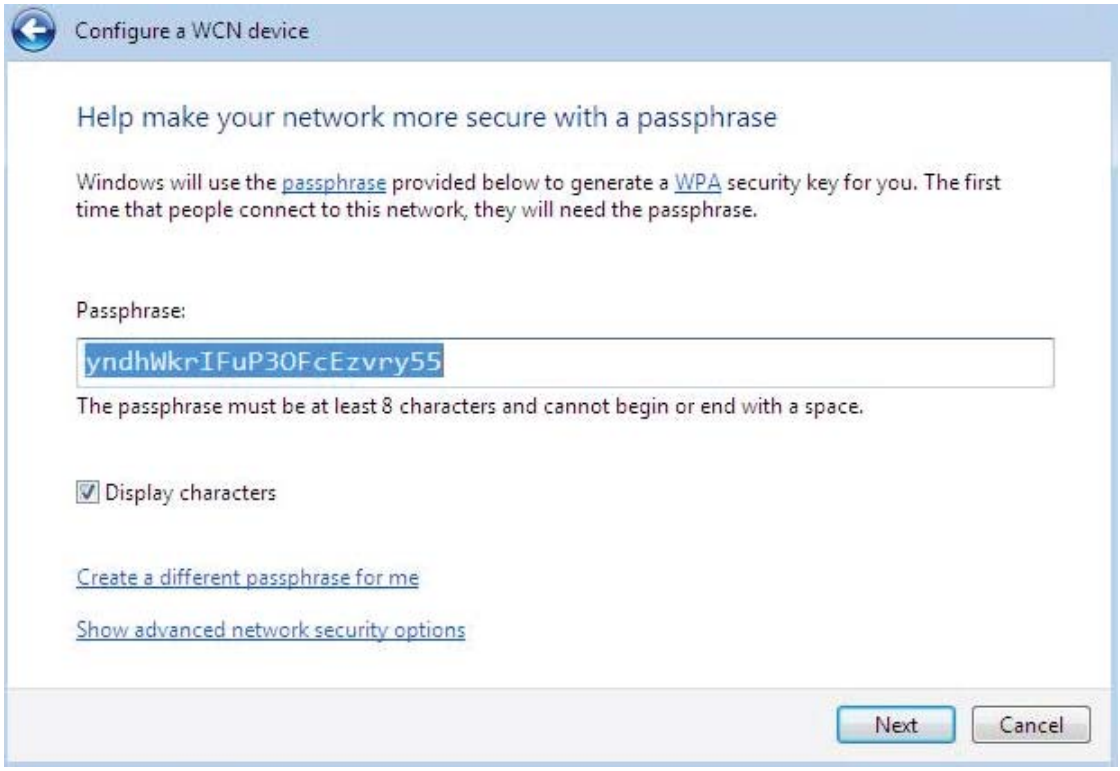
2. Access the Control Panel page (Start > Control Panel). Select Network and Internet > View Network computers and devices. Double click the ADSL Firewall Router icon and then enter the AP PIN code and press Next.

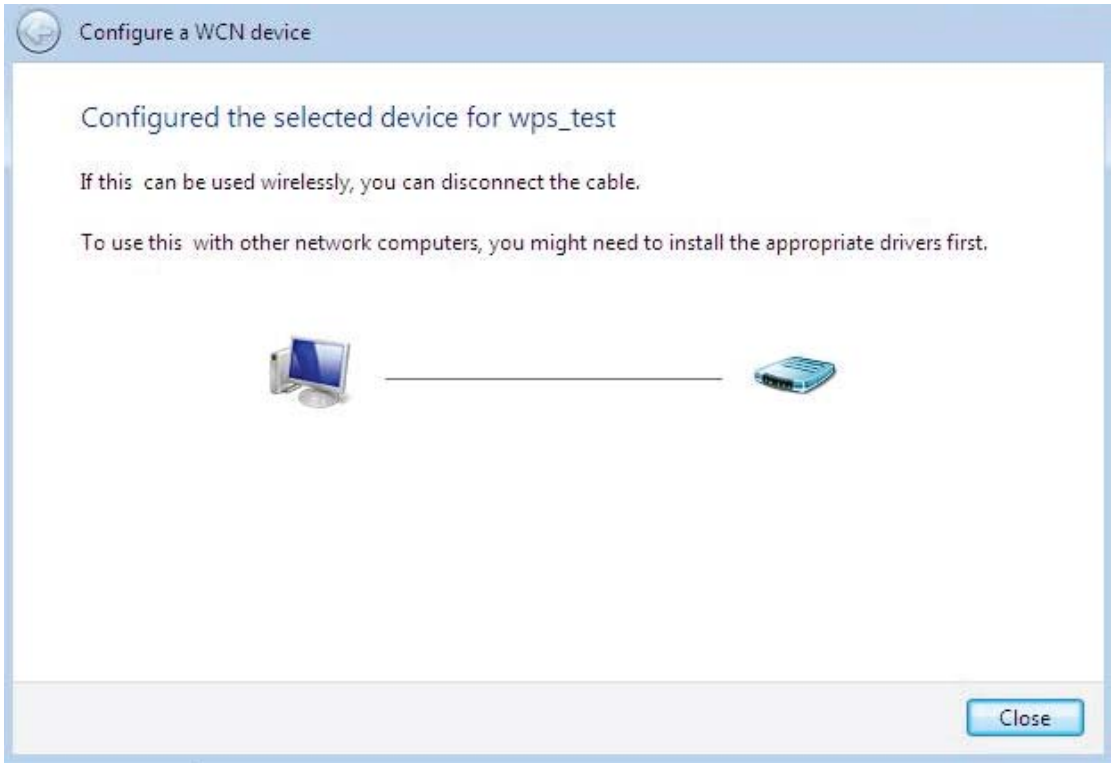


3. Enter the AP SSID and click Next.



4. Enter the Passphrase and click Next to complete the setup.


Configure a WCN device
Help make your network more secure with a passphrase
Windows will use the passphrase provided below to generate a WPA security key for you. The first time that people connect to this network, they will need the passphrase.
Passphrase:
yndhWkrIFuP3OFcEzvry55
The passphrase must be at least 8 characters and cannot begin or end with a space.
Display characters
Create a different passphrase for me
Show advanced network security options
Next
Cancel

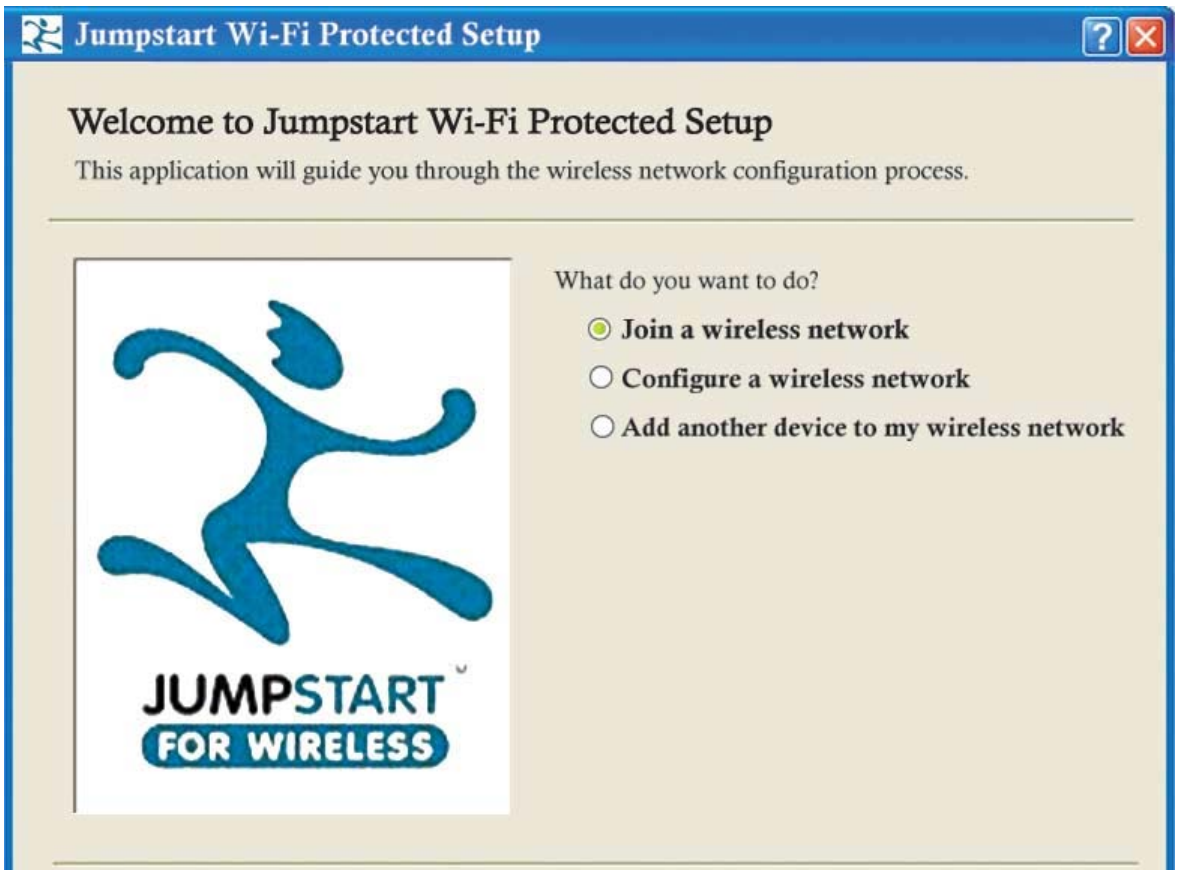

Configure a WCN device
Configured the selected device for wps_test
If this can be used wirelessly, you can disconnect the cable.
To use this with other network computers, you might need to install the appropriate drivers first.
Close

Adding a new WPS device (wireless client) to the network - PBC Method

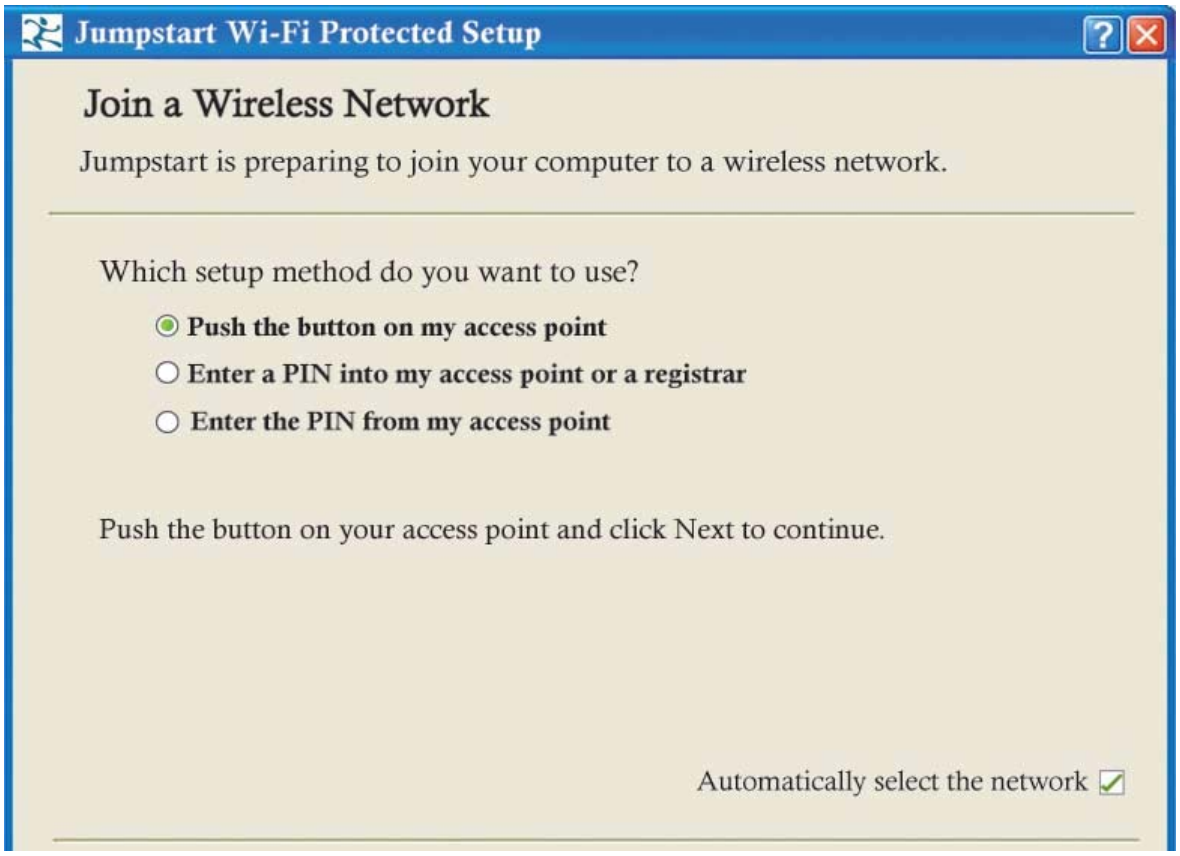
1. Push the WPS button for more than 1 second until the wireless LED flashes.

Note: Once the WPS button is pushed, steps 2 & 3 should be completed within 2 minutes.

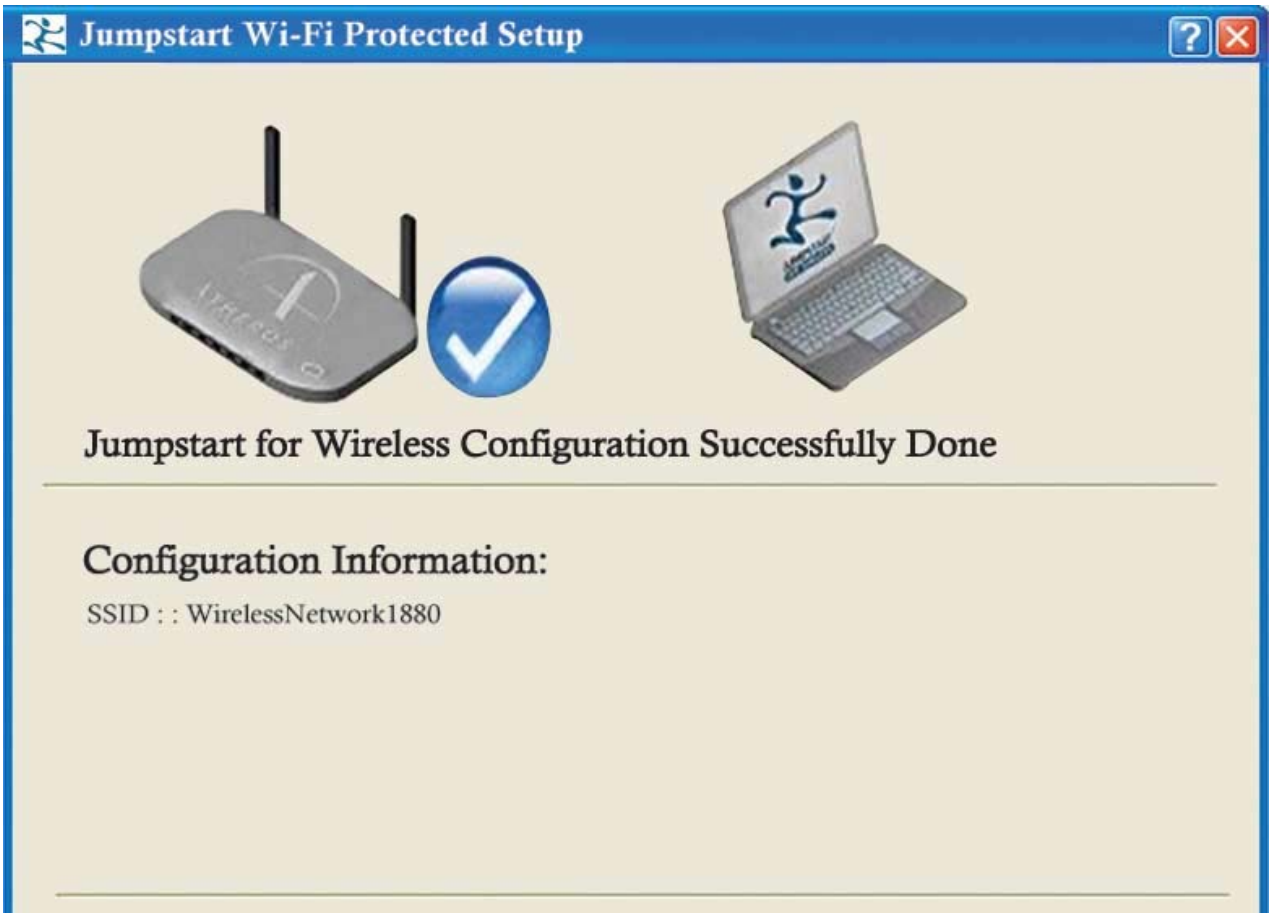
2. Access the client's WPS utility, select Join a Wireless Network and then click Next.


Jumpstart Wi-Fi Protected Setup
Welcome to Jumpstart Wi-Fi Protected Setup
This application will guide you through the wireless network configuration process.
What do you want to do?
Join a wireless network
Configure a wireless network
Add another device to my wireless network
JUMPSTART
FOR WIRELESS

3. Select Push the button on my access point and click Next.

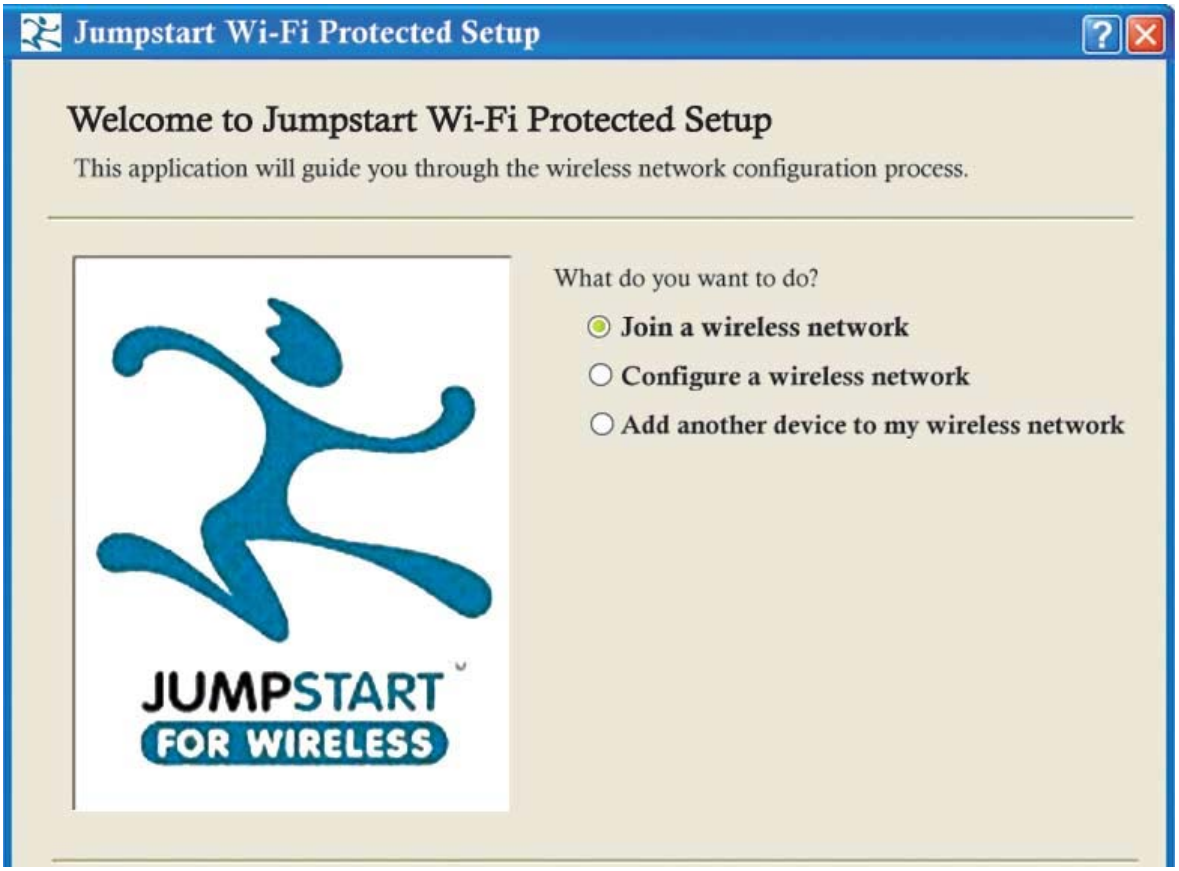

Jumpstart Wi-Fi Protected Setup
Join a Wireless Network
Jumpstart is preparing to join your computer to a wireless network.
Which setup method do you want to use?
Push the button on my access point
Enter a PIN into my access point or a registrar
Enter the PIN from my access point
Push the button on your access point and click Next to continue.
Automatically select the network

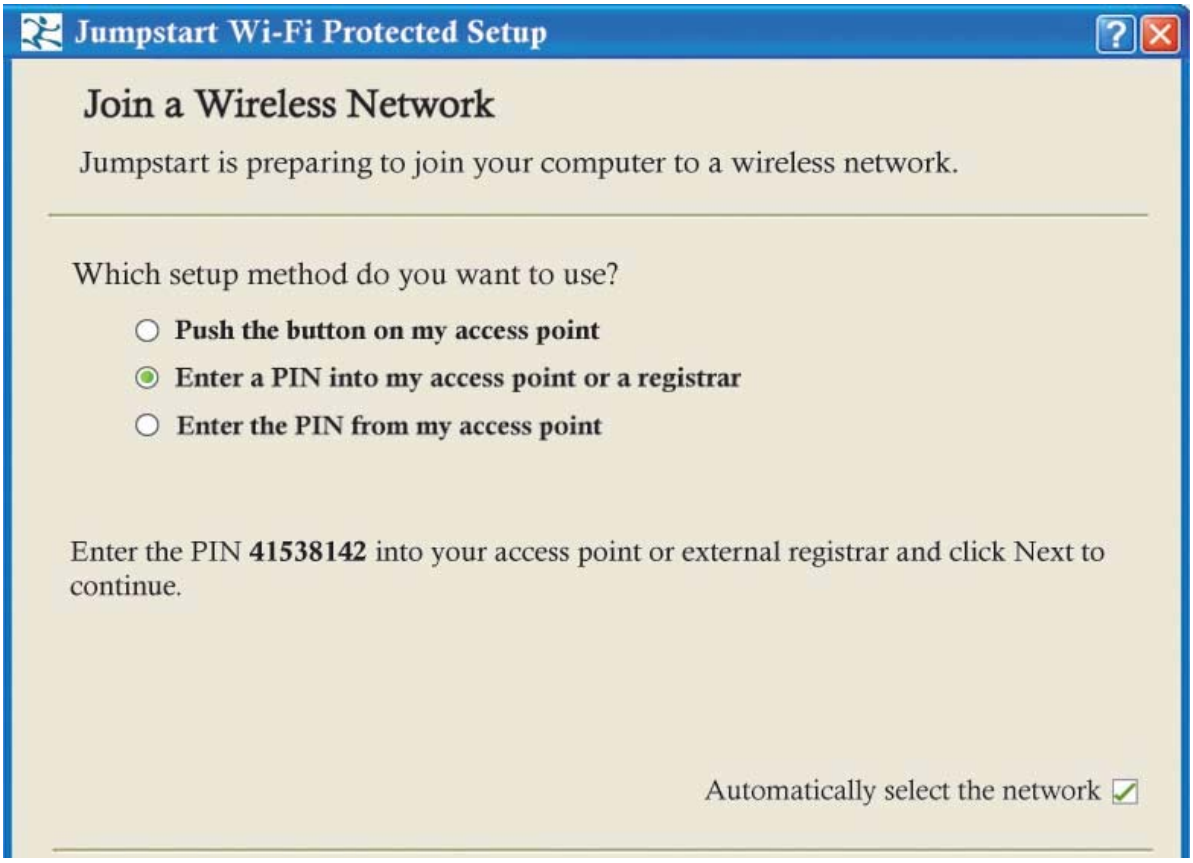
4. Your device will now be joined to the wireless network.


Jumpstart Wi-Fi Protected Setup
Jumpstart for Wireless Configuration Successfully Done
Configuration Information:
SSID : : WirelessNetwork1880

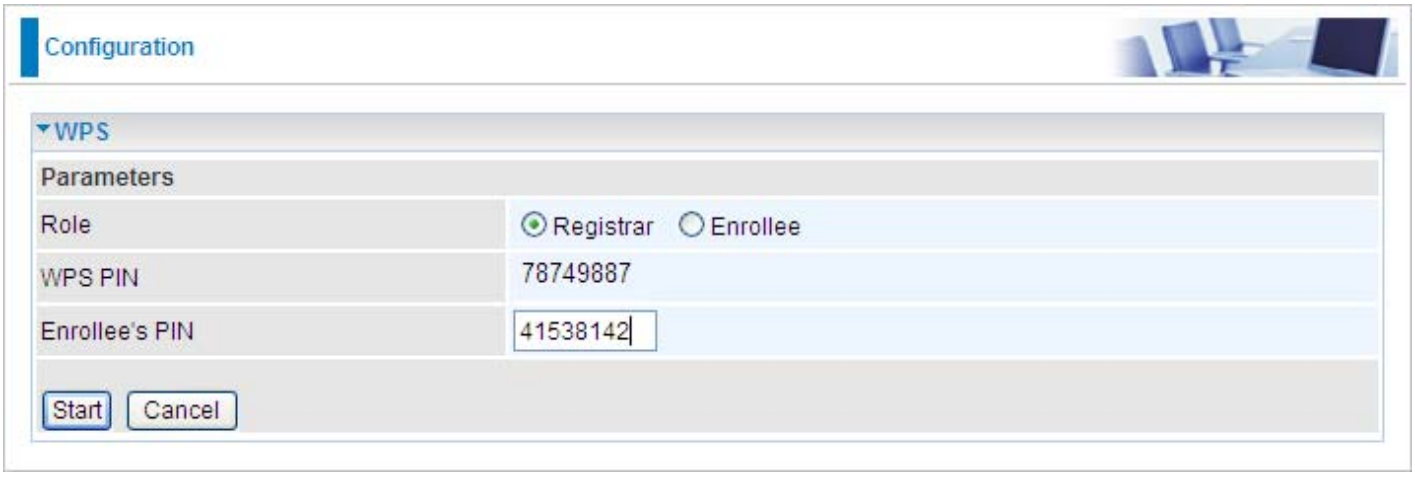
Adding a new WPS device (wireless client) to the network - PIN Method

1. Access the client's WPS utility, select Join a Wireless Network and then click Next.
2. Select Enter a PIN into my access point or a registrar. Then jot down the PIN number (eg. 41538142) before pressing Next to activate the wireless client WPS PIN method.

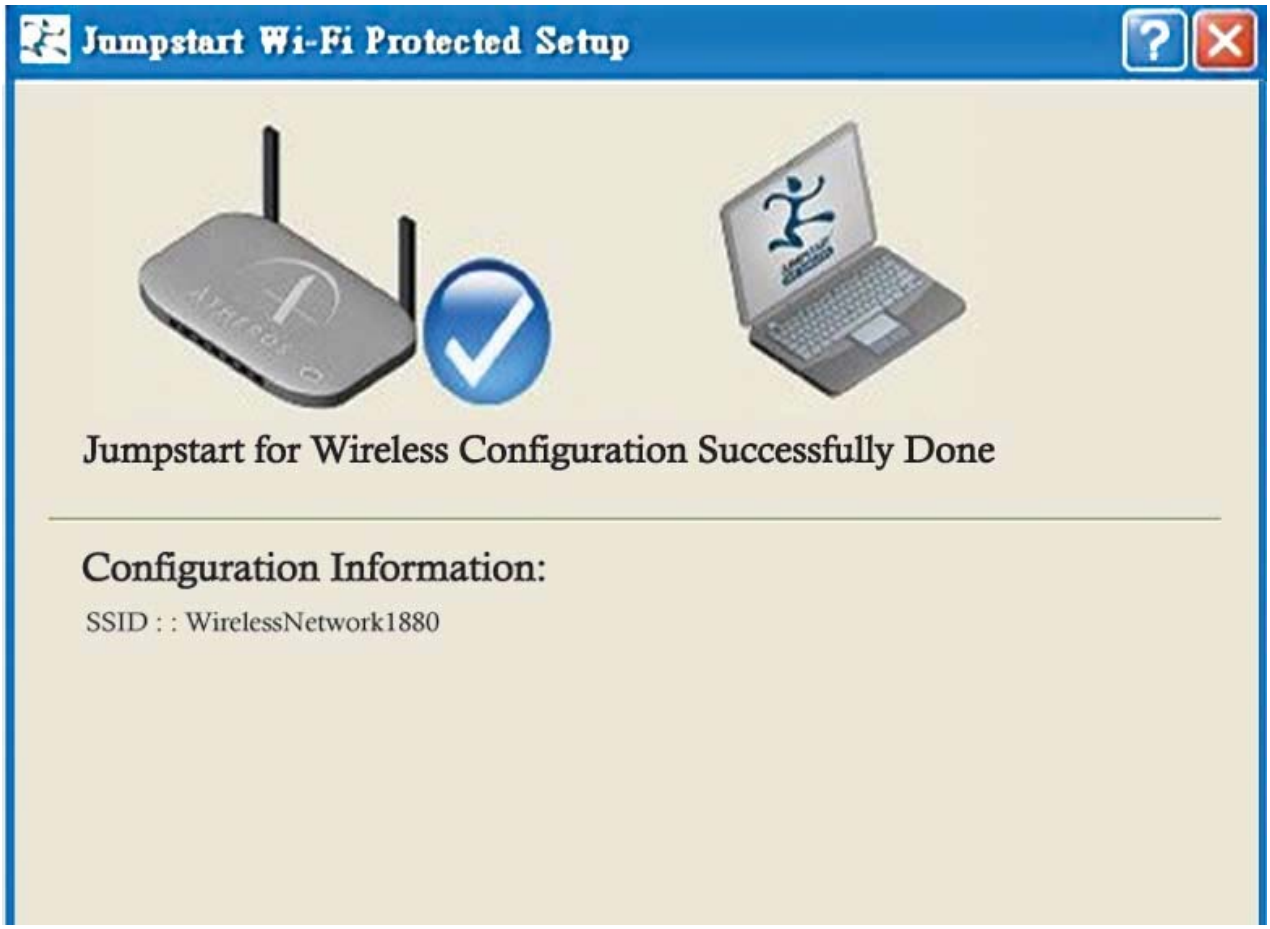

Jumpstart Wi-Fi Protected Setup
Welcome to Jumpstart Wi-Fi Protected Setup
This application will guide you through the wireless network configuration process.
JUMPSTART
FOR WIRELESS
What do you want to do?
Join a wireless network
Configure a wireless network
Add another device to my wireless network


Jumpstart Wi-Fi Protected Setup
Join a Wireless Network
Jumpstart is preparing to join your computer to a wireless network.
Which setup method do you want to use?
Push the button on my access point
Enter a PIN into my access point or a registrar
Enter the PIN from my access point
Enter the PIN 41538142 into your access point or external registrar and click Next to continue.
Automatically select the network

3. Access the WPS Web GUI, and enter the PIN number that you have previously jotted down into the Enrollee PIN column. When it is done, press Start.

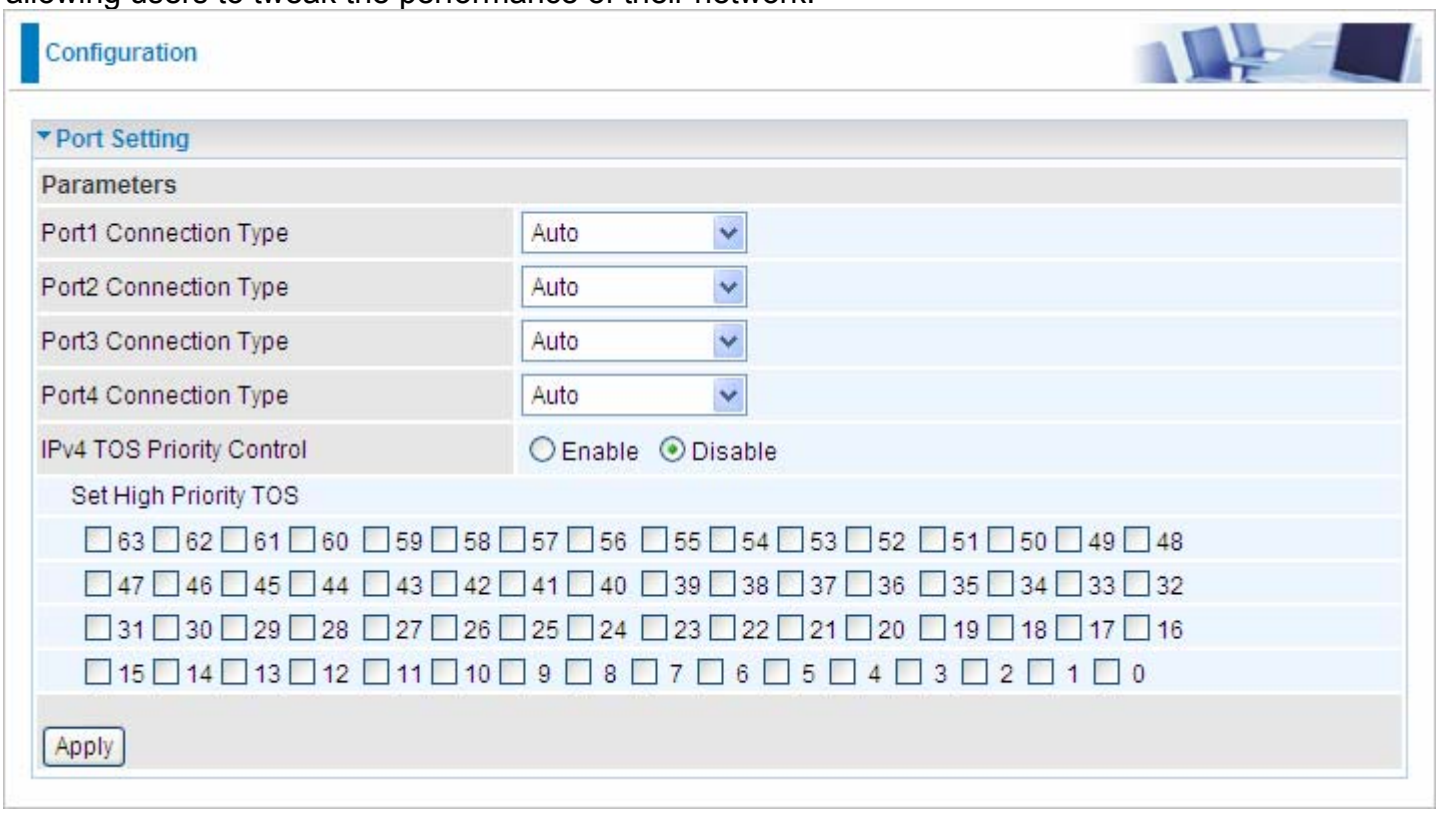


4. By now you should have your device joined with a wireless network.


Jumpstart Wi-Fi Protected Setup
Jumpstart for Wireless Configuration Successfully Done
Configuration Information:
SSID : : WirelessNetwork1880

Port Setting

This section allows you to configure the settings for the router's Ethernet ports to solve some of the compatibility problems that may be encountered while connecting to the Internet, as well allowing users to tweak the performance of their network.


Configuration
Port Setting
Parameters
Port1 Connection Type
Auto
Port2 Connection Type
Auto
Port3 Connection Type
Auto
Port4 Connection Type
Auto
IPv4 TOS Priority Control
Enable
Disable
Set High Priority TOS
63 62 61 60 59 58 57 56 55 54 53 52 51 50 49 48
47 46 45 44 43 42 41 40 39 38 37 36 35 34 33 32
31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16
15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Apply

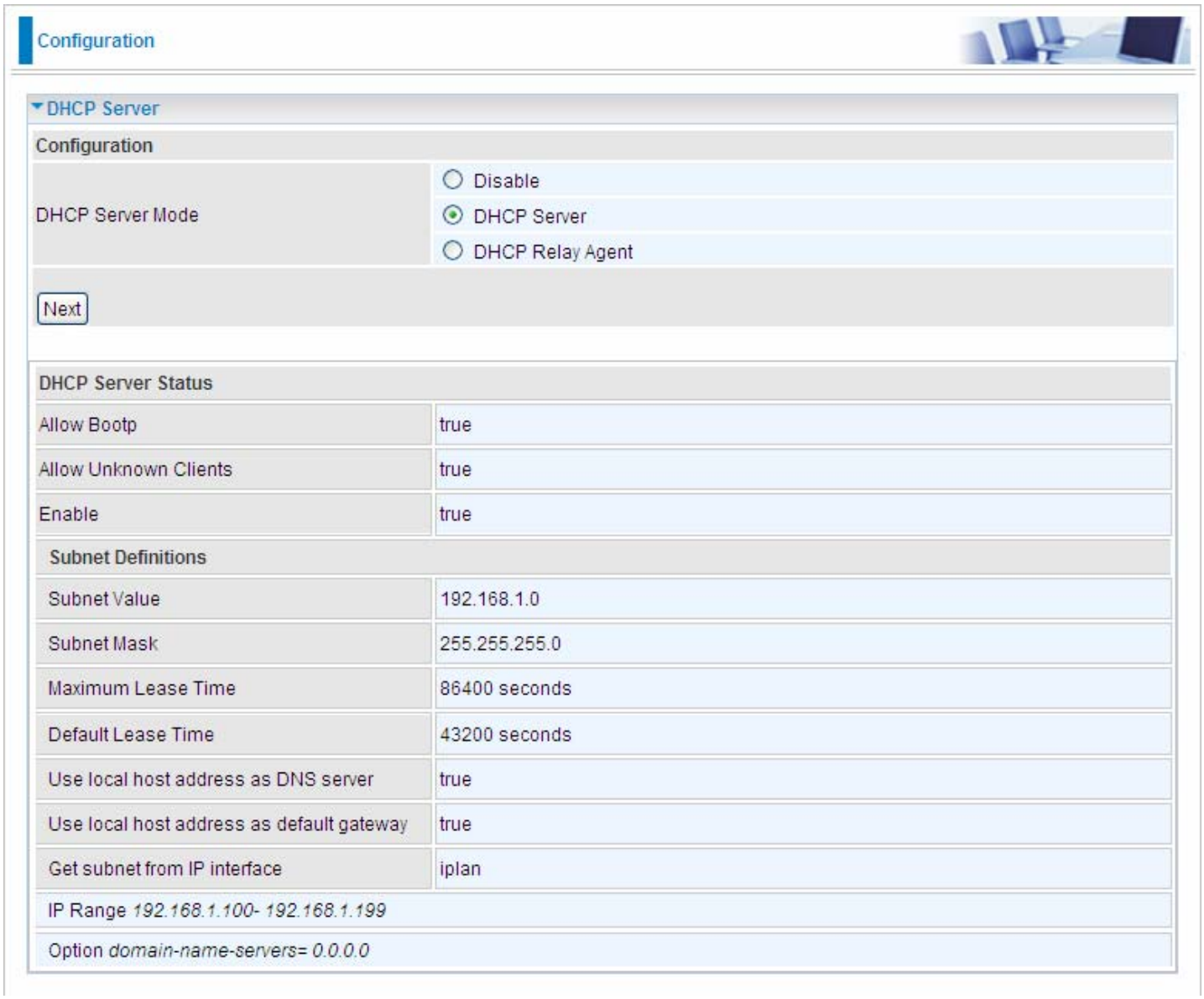
Port # Connection Type: There are Six options to choose from: Auto, disable, 10M half-duplex, 10M full-duplex, 100M half-duplex, 100M full-duplex and Disable. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices, and you can configure different types to solve compatibility issues. The default is Auto, which users should keep unless there are specific problems with PCs not being able to access your LAN.

IPv4 TOS priority Control (Advanced users): TOS, Type of Services, is the 2nd octet of an IP packet. Bits 6-7 of this octet are reserved and bit 0-5 are used to specify the priority of the packet.

This feature uses bits 0-5 to classify the packet's priority. If the packet priority is set as high, its transmission will be given the first priority it will not be constrained by the Rate Limit. Therefore, when this feature is enabled, the router's Ethernet switch will first check the 2nd octet of each IP packet. If the value in the TOS field matches the values checked in the table (0 to 63), this packet will be treated as high priority.

DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to the PCs on your network if they are configured to obtain IP addresses automatically.



To disable the router DHCP Server, check Disabled and click Next, then click Apply. When the DHCP Server is disabled you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (by default this is 192.168.1.254).

To configure the router DHCP Server, check DHCP Server and click Next. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click Apply to enable this function. If you check Use Router as a DNS Server", the Router will perform the domain name lookup, find the IP address from the outside network automatically and forward it back to the requesting PC in the LAN (your Local Area Network).

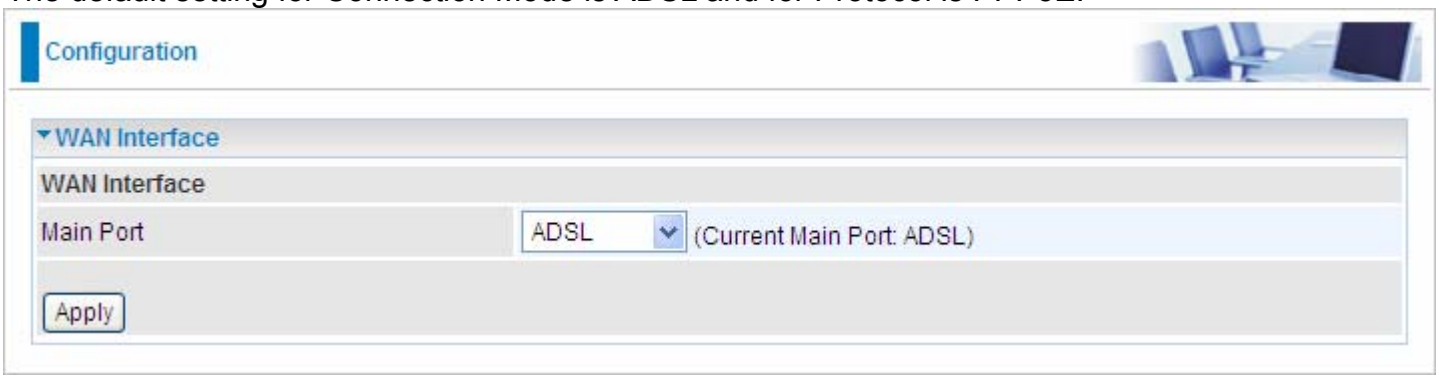
If you check DHCP Relay Agent and click Next, then you will have to enter the IP address of the DHCP server which will assign an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP.
Click Apply to enable this function.

WAN - Wide Area Network

WAN refers to your Wide Area Network connection, i.e. your router's connection to your ISP and Internet. Here are the items within the WAN section: **WAN Interface**, **WAN Profile** and **ADSL Mode**.

WAN Interface

The default setting for Connection Mode is ADSL and for Protocol is PPPoE.

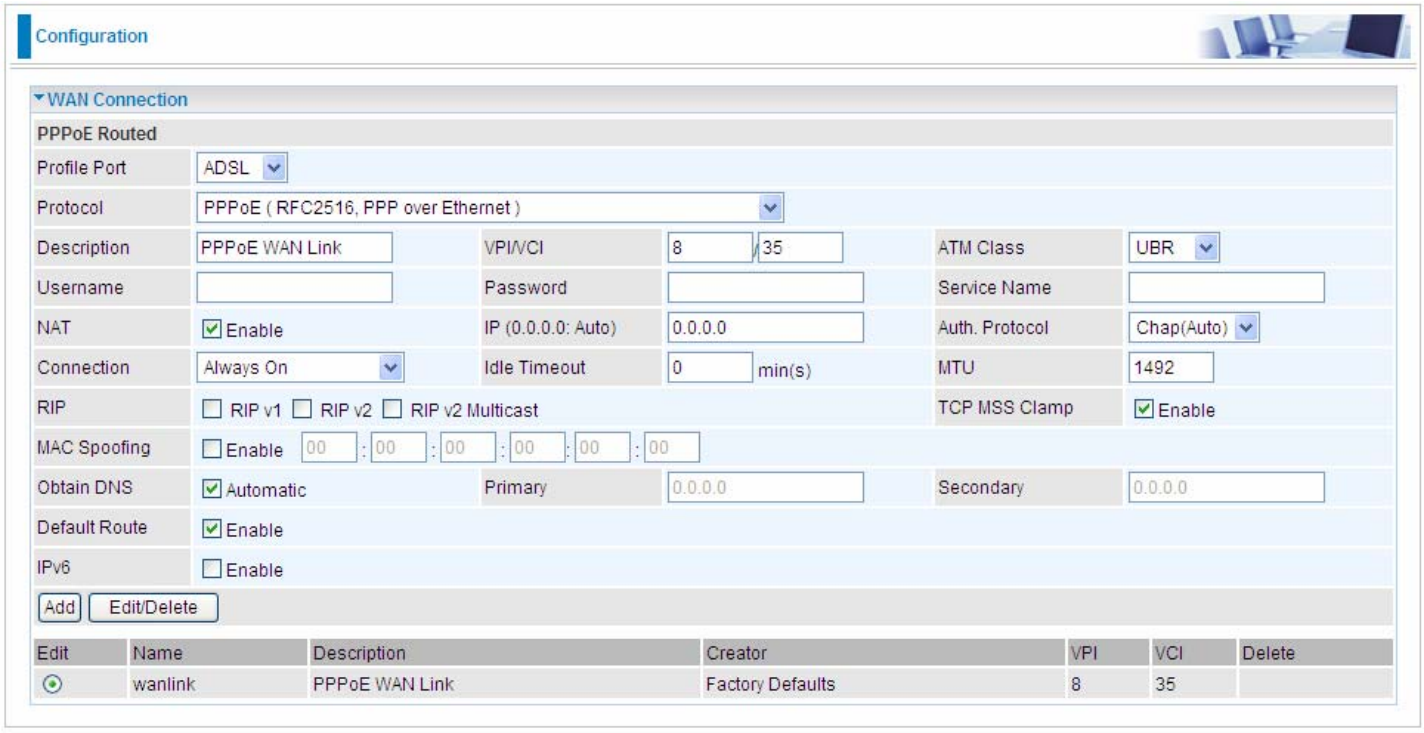


Main Port: User can select either ADSL, EWAN or Dual WAN mode.

WAN Profile

PPPoE Connection

PPPoE (PPP over Ethernet) provides access control in a manner which is similar to dial-up services using PPP.



Profile Port: Select the profile port as ADSL.

Protocol: The ATM protocol will be used in the device.

Description: A given name for the connection.

VPI/VCI: Enter the information provided by your ISP. **ATM Class:** The Quality of Service for ATM

layer.

Username: Enter the username provided by your ISP. You can input up to 128 alpha-numeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 128 alpha-numeric characters (case sensitive).

Service Name: This item is for identification purpose. If it is required, your ISP will provide you the information. Maximum input is 15 alpha-numeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP (0.0.0.0:Auto): Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

Auth. Protocol: Default is Auto. Your ISP should advise you on whether to use Chap or Pap.
Connection:

Always on: If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

Connect on Demand: If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the router when there is no activity on the line for a predetermined period of time.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

MAC Spoofing: Some service providers require the configuring of this option. You must fill in the MAC address that is specified by the service provider when it is required. Default is disabled.

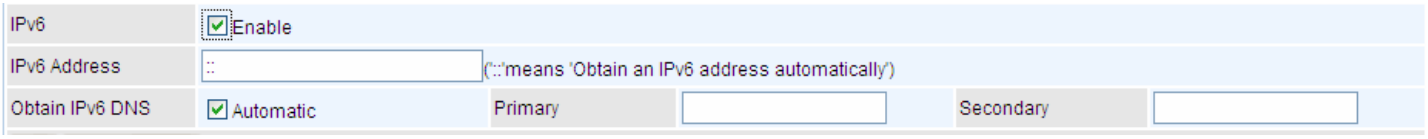
Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Default Route: Check to enable default route.

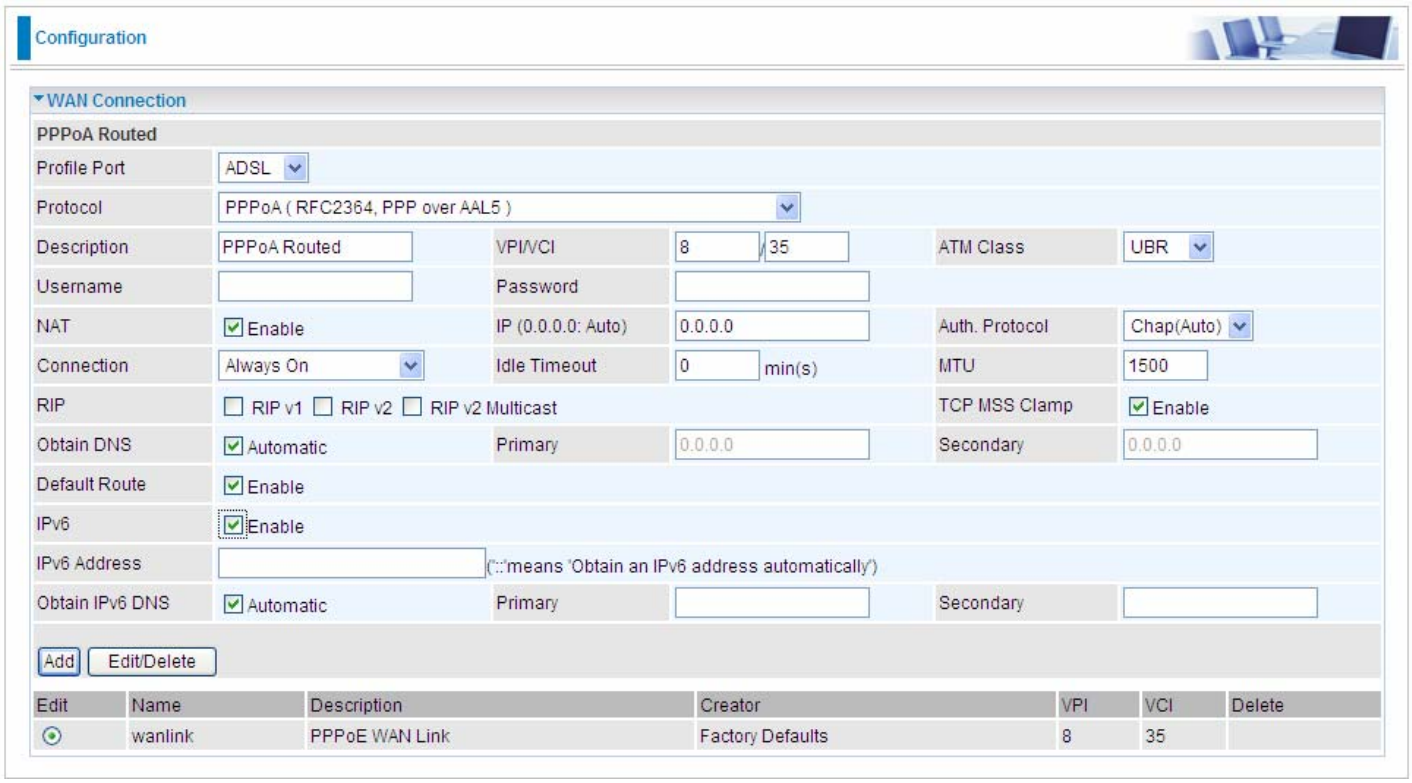
IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.



IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ” ::” means to obtain IPv6 address automatically.

Obtain IPv6 DNS: check **Automatic** to obtain DNS automatically. If not, please type the concrete one in the Primary field.

PPPoA Connection



Profile Port: Select the profile port as ADSL.

Protocol: The ATM protocol will be used in the device..

Description: A given name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

Username: Enter the username provided by your ISP. You can input up to 128 alpha-numeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 128 alpha-numeric characters (case sensitive).

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP

addresses and can access the Internet directly, the NAT function can be disabled.

IP (0.0.0.0:Auto): Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

Auth. Protocol: Default is Auto. Your ISP should advise you on whether to use Chap or Pap.

Connection:

Always on: If you want the router to establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.

Connect on Demand: If you want to establish a PPPoA session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the router when there is no activity on the line for a predetermined period of time.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

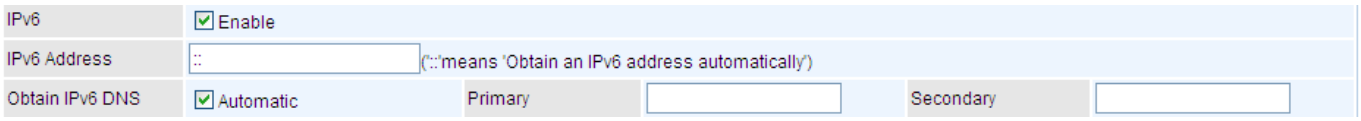
Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Default Route: Check to enable default route.

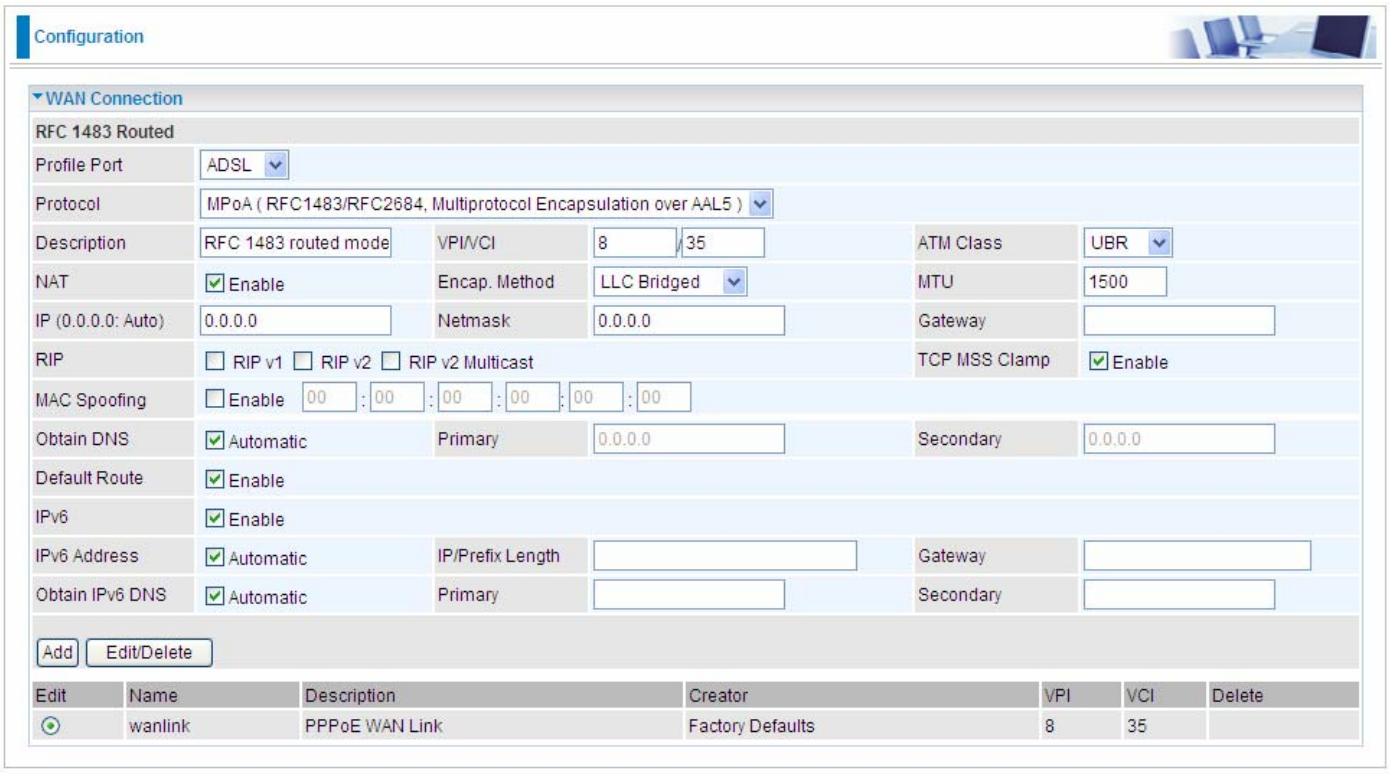
IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.



IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ” ::” means to obtain IPv6 address automatically.

Obtain IPv6 DNS: check **Automatic** to obtain DNS automatically. If not, please type the concrete one in the Primary field.

MPoA Connection



Profile Port: Select the profile port as ADSL.

Protocol: The ATM protocol will be used in the device.

Description: A given name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Encap. Method: Choose whether you want the packets in WAN interface as bridged packet or routed packet.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

IP (0.0.0.0:Auto): Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

Netmask: The default is 255.255.255.0. User can change it to other such as 255.255.255.128. Type the subnet mask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway (if given).

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

MAC Spoofing: Some service providers require the configuring of this option. You must fill in the MAC address that is specified by the service provider when it is required. Default is disabled.

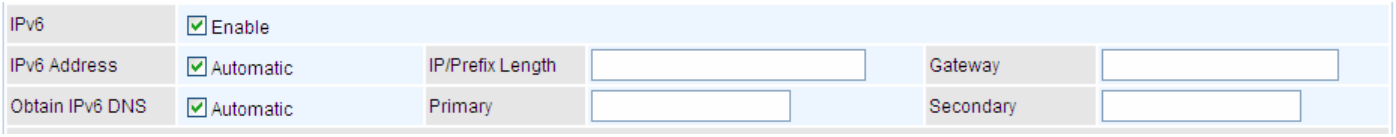
Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Default Route: Check to enable default route.

IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.

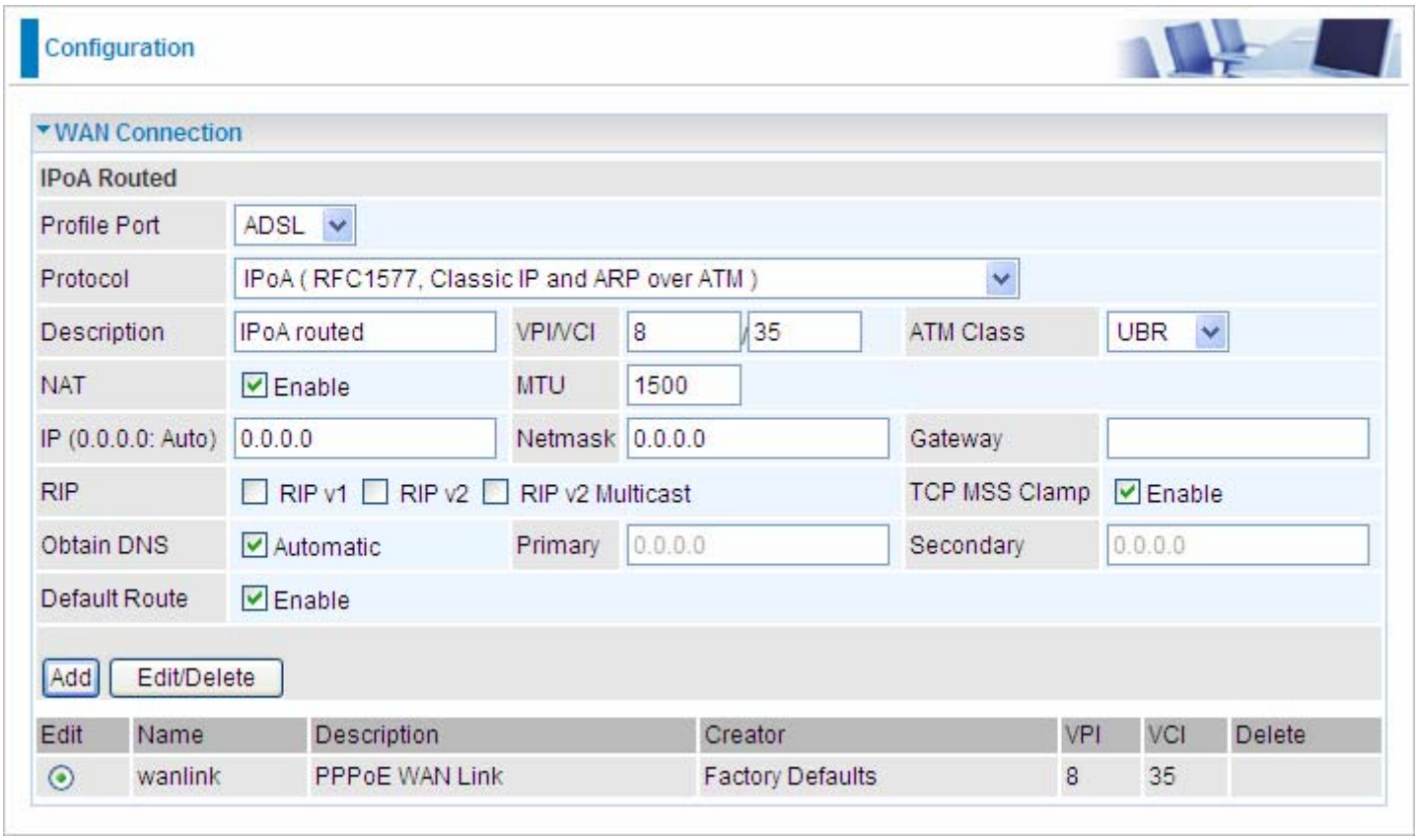


IPv6 Address: Check **Automatic** to obtain IPv6 address automatically. If not, please type the IP and the prefix length for the IPv6 address from your ISP.

Gateway: Type the gateway to which the WAN packets are forwarded.

Obtain IPv6 DNS: check **Automatic** to obtain DNS automatically. If not, please type the concrete one in the Primary field.

IPoA Routed Connection



Profile Port: Select the profile port as ADSL.

Protocol: The ATM protocol will be used in the device.

Description: A given name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

IP (0.0.0.0:Auto): Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

Netmask: The default is 255.255.255.0. User can change it to other such as 255.255.255.128. Type the subnet mask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway (if given).

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

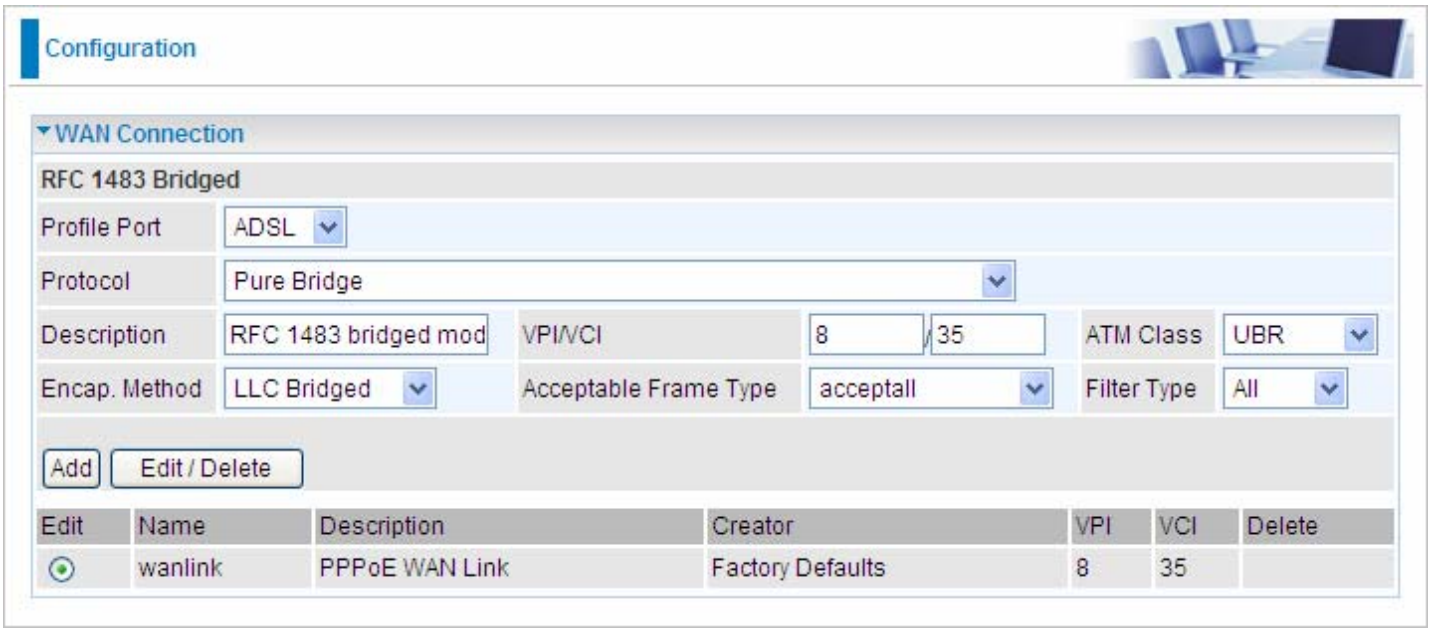
Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Default Route: Check to enable default route.

Pure Bridge



Profile Port: Select the profile port as ADSL.

Protocol: The ATM protocol will be used in the device.

Description: A given name for this connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

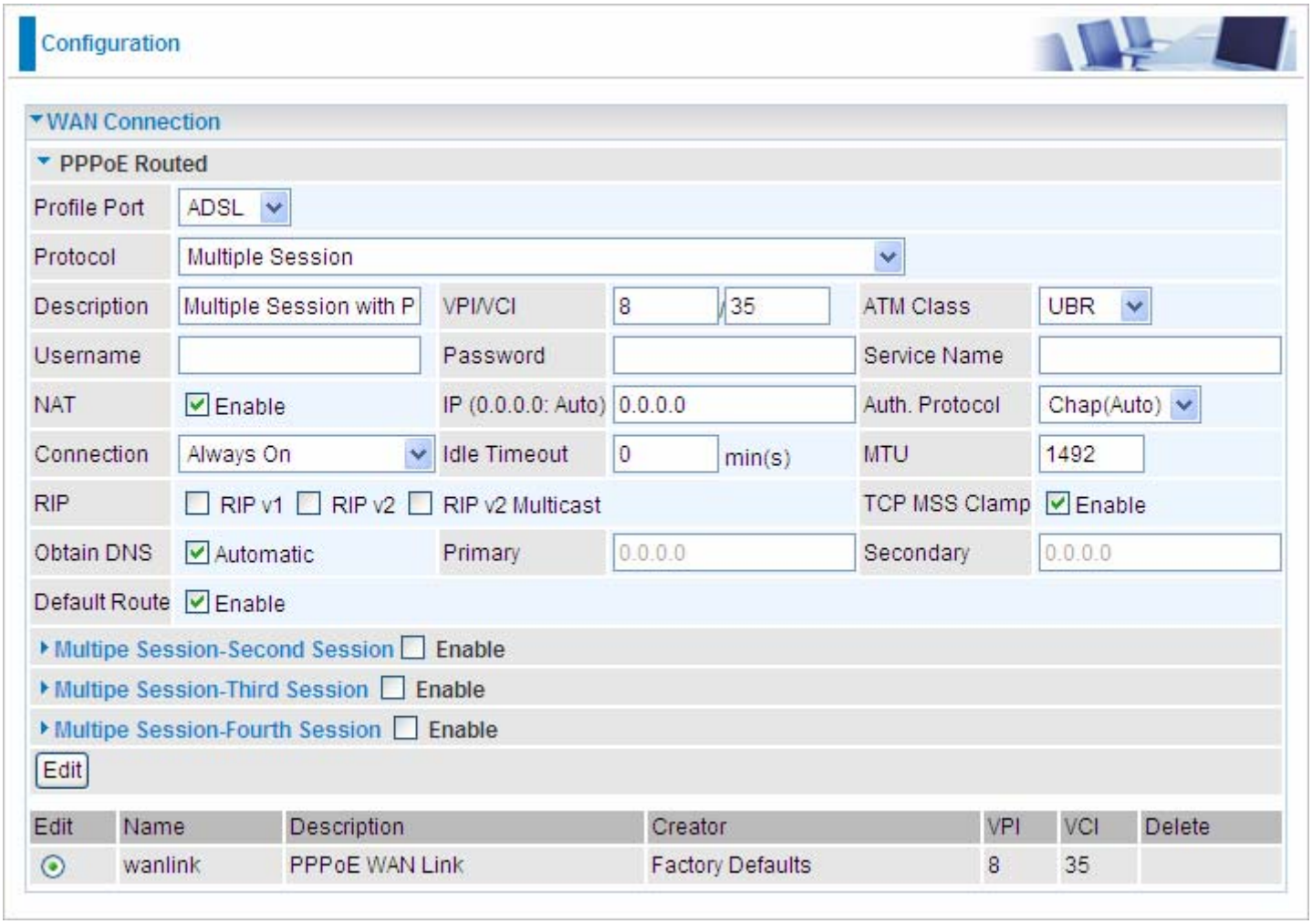
Encap. Method: Choose whether you want the packets in WAN interface as bridged packet or routed packet.

Acceptable Frame Type: Specify which kind of traffic goes through this connection, all traffic or only VLAN tagged.

Filter Type: Specify the type of ethernet filtering performed by the named bridge interface.

All	Allows all types of ethernet packets through the port.
Ip	Allows only IP/ARP types of ethernet packets through the port.
Pppoe	Allows only PPPoE types of ethernet packets through the port.

Multiple Session



Profile Port: Select the profile port as ADSL.

Protocol: The Multiple Session protocol will be used in the device.

Description: A given name for this connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

Username: Enter the username provided by your ISP. You can input up to 128 alpha-numeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 128 alpha-numeric characters (case sensitive).

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP (0.0.0.0:Auto): Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

Auth. Protocol: Default is Auto. Your ISP should advise you on whether to use Chap or Pap.

Connection:

Always on: If you want the router to establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.

Connect on Demand: If you want to establish a PPPoA session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the router when there is no activity on the line for a predetermined period of time.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

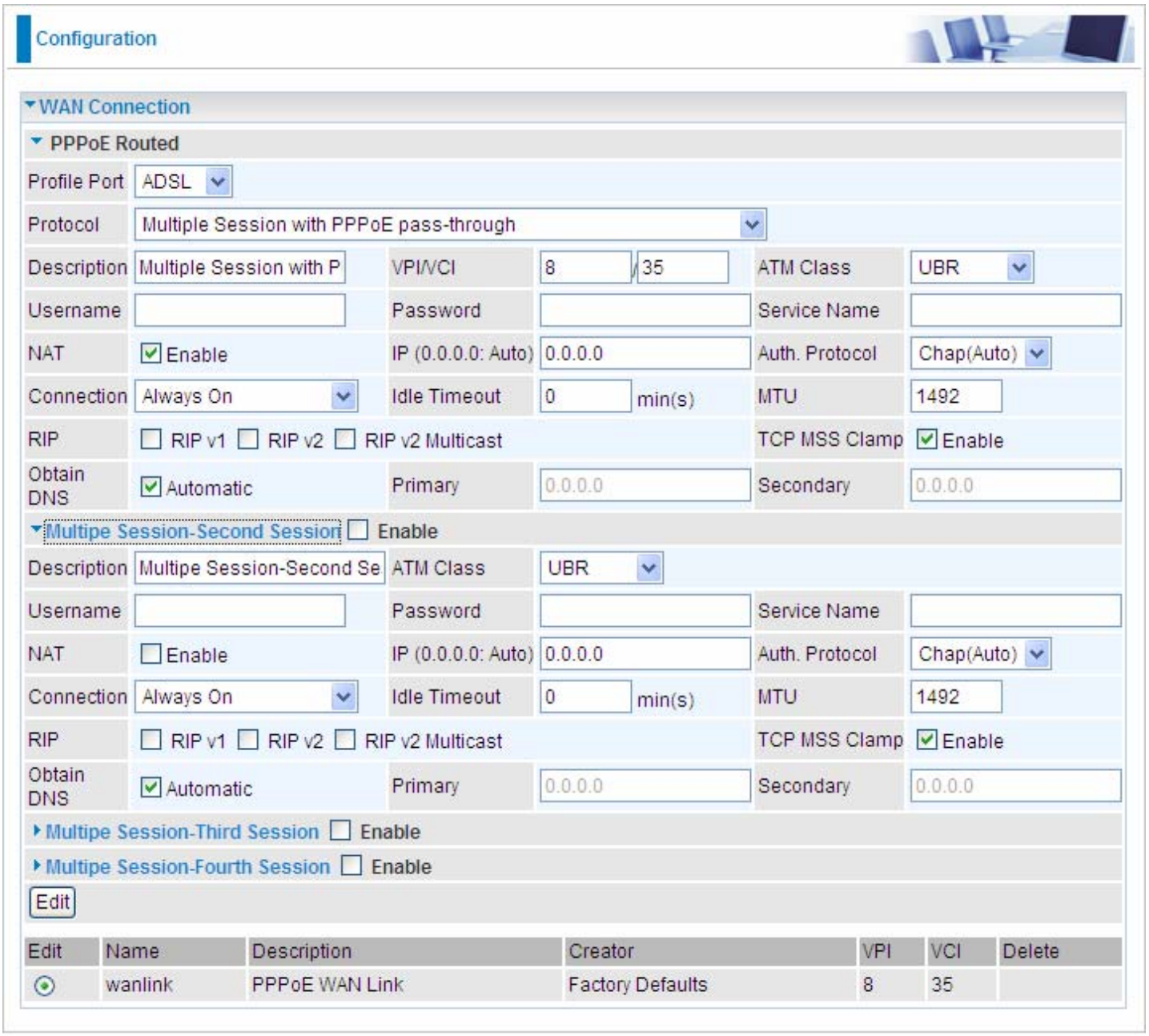
Secondary DNS: Enter the secondary DNS.

Default Route: Check to enable default route.

Multiple Session Second Session / Multiple Session Third Session / Multiple Session Forth Session: Check Enable to activate the second/third/forth session.

If you want to establish several connections at the same time, check **Enable** to enable the second, third or fourth connection.

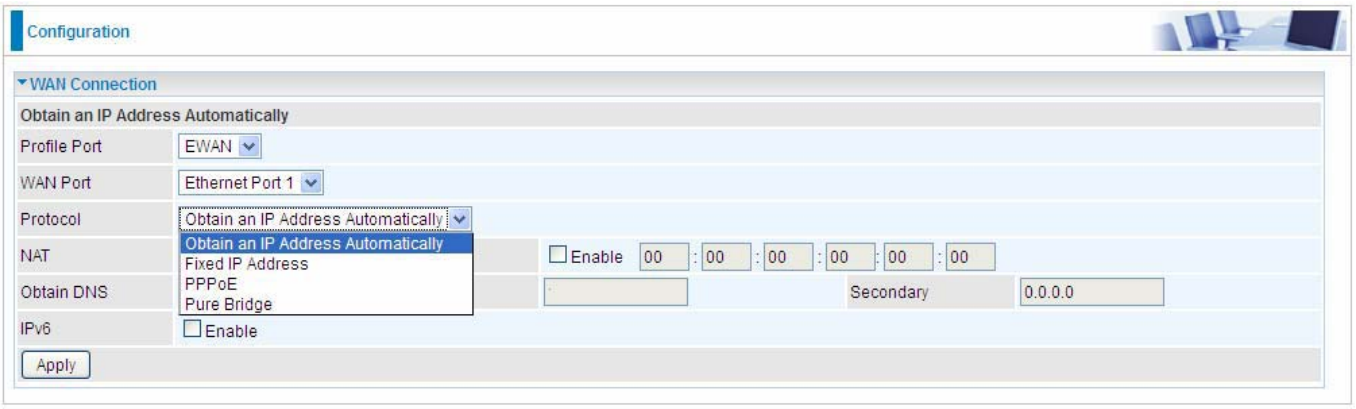
Before this, you need to configure your second, third or fourth connection firstly. Click **Multiple Session-Second Session,** the following screen will appear:



Configure the detailed information for your second connection like the previous one.

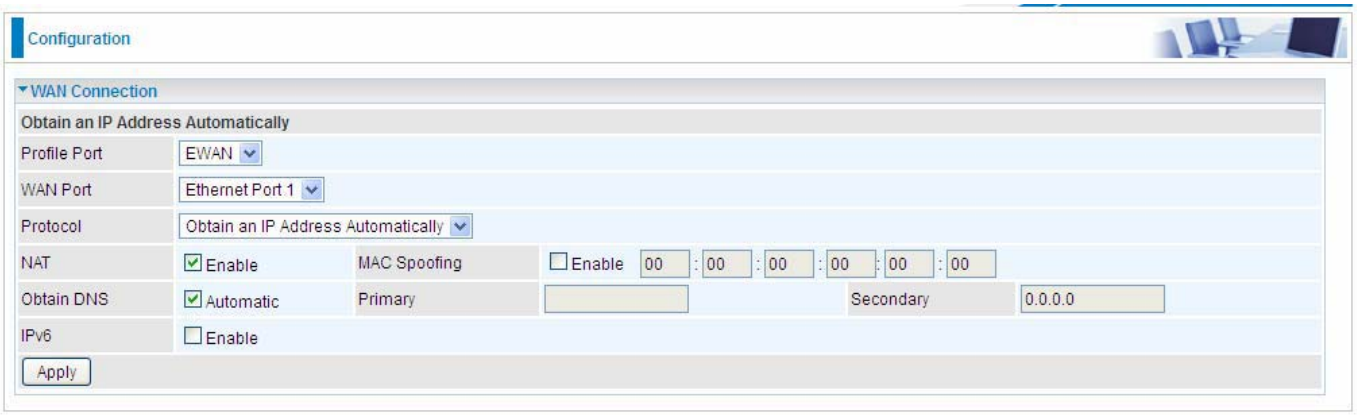
EWAN

In EWAN mode, LAN 1 port will be configured as EWAN port for connecting to Internet.



Protocol: You can select one of four protocols for the router's WAN settings: **Obtain an IP Address Automatically, Fixed IP Address, PPPoE, Pure Bridge**.

1. Obtain an IP Address Automatically: Select this item if the device is connected to a router that has DHCP functionality enabled.

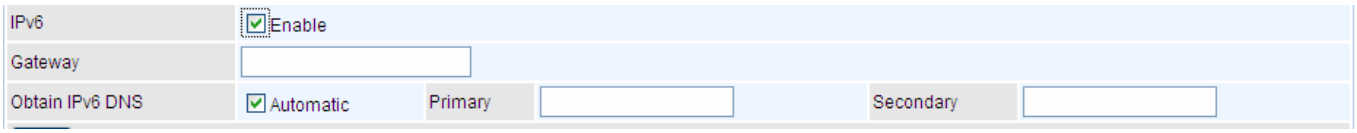


NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If PCs in LAN should share the WAN IP for WAN access, please enable NAT. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router's MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

Obtain DNS: Check the **Automatic** to enable the router to configure this value, or type in the Primary and Secondary DNS values provided by your ISP.

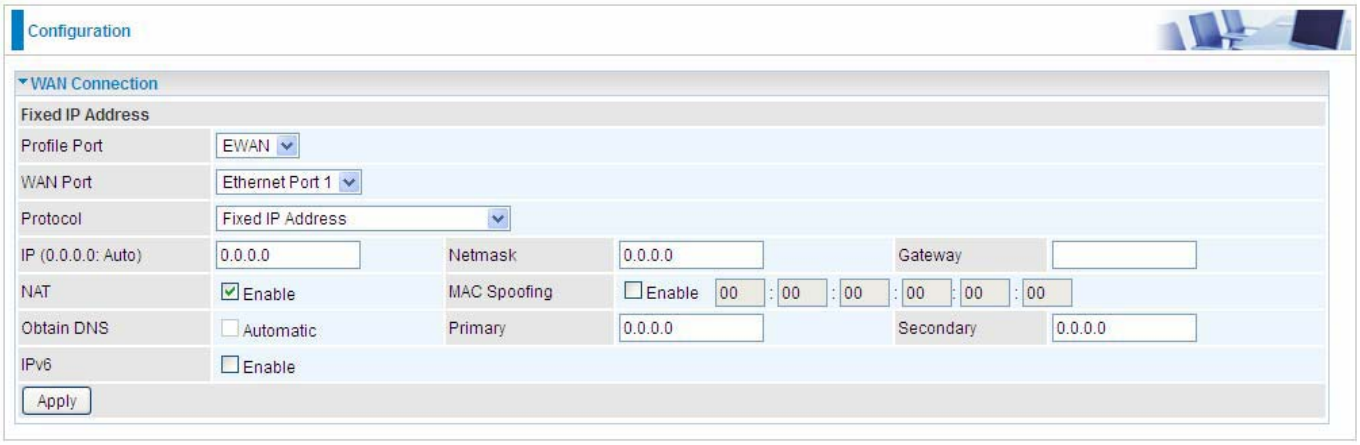
IPv6: check to enable IPv6 service. Enter IPv6 Gateway address and set IPv6 DNS as same in IPv4 mode.



Gateway: type the gateway address to which WAN packets are forwarded.

Obtain IPv6 DNS: check **Automatic** to obtain DNS automatically. If not, please type the concrete ones in the Primary and Secondary field.

2. Fixed IP Address: Select this item if your ISP provides you with a static IP address.



IP(0.0.0.0: Auto): Type the IP address that your ISP provided.

Netmask: Type the subnet mask that your ISP provided. **Gateway:** Type the gateway address that your ISP provided.

Gateway: You must specify a gateway IP address (supplied by your ISP).

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If PCs in LAN should share the WAN IP for WAN access, please enable NAT. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router's MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

Obtain DNS: Check the **Automatic** to enable the router to configure this value, or type in the Primary and Secondary DNS values provided by your ISP.

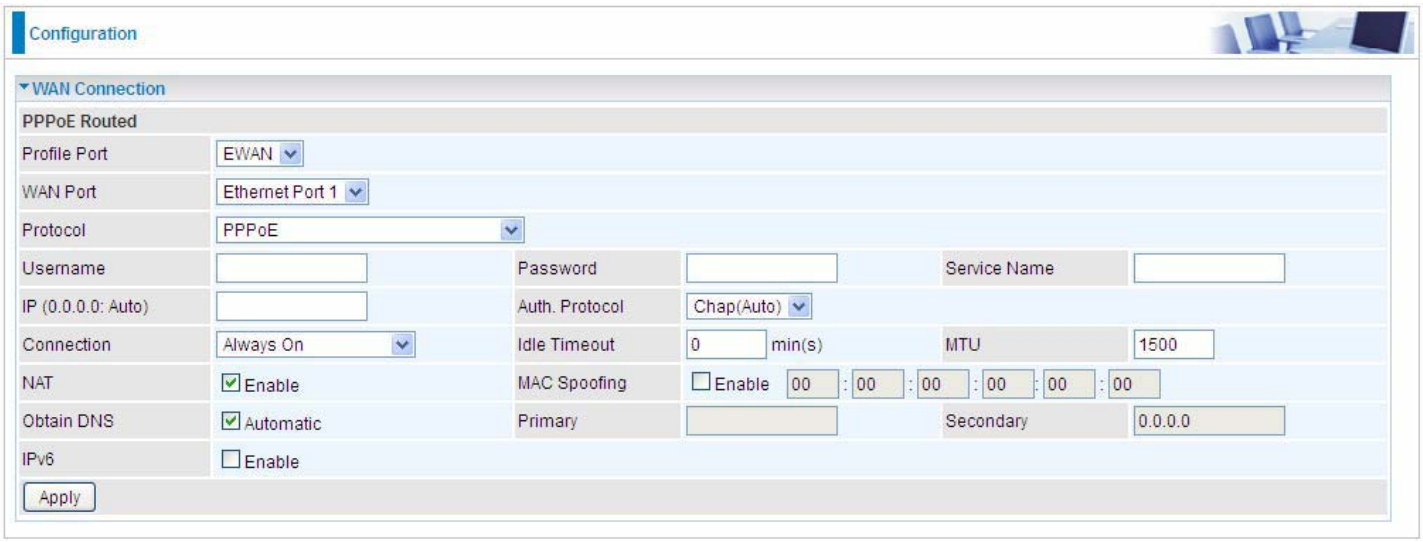
IPv6: check to enable IPv6 service. Enter IPv6 Gateway address and set IPv6 DNS as same in IPv4 mode.

IP/Prefix Length: Please specify the IP and the prefix length for the IPv6 address from your ISP.

Gateway: Type the gateway to which the WAN packets are forwarded.

Obtain IPv6 DNS: check **Automatic** to obtain DNS automatically. If not, please type the concrete one in the Primary field.

3. PPPoE: Select this item if your ISP uses the PPPoE protocol.



Username: Enter the username provided by your ISP. You can input up to 128 alphanumeric characters(case sensitive). This is in the format of “username@ispname“ instead of simply “username“.

Password: Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is 15 alphanumeric characters.

IP (0.0.0.0: Auto): Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

Auth Protocol: Default is Auto. Your ISP should advise you on whether to use Chap or Pap.

Connection: If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP, please select **Always on**. If you want to establish a PPPoE session only when there is a packet requesting access to Internet (i.e. when a program on your computer attempts to access the Internet), please select **Connect on Demand**.

Idle Timeout: Auto-disconnect the router when there is no activity on the line for a predetermined period of time.

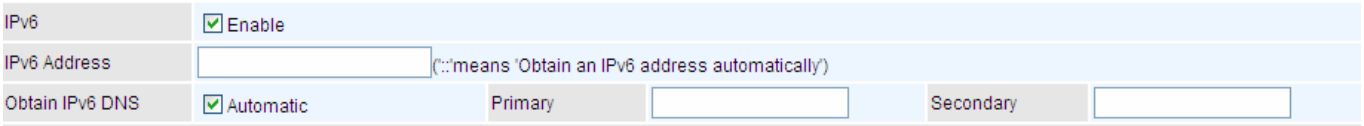
MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If PCs in LAN should share the WAN IP for WAN access, please enable NAT. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router’s MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

Obtain DNS: Check the **Automatic** to enable the router to configure this value, or type in the Primary and Secondary DNS values provided by your ISP.

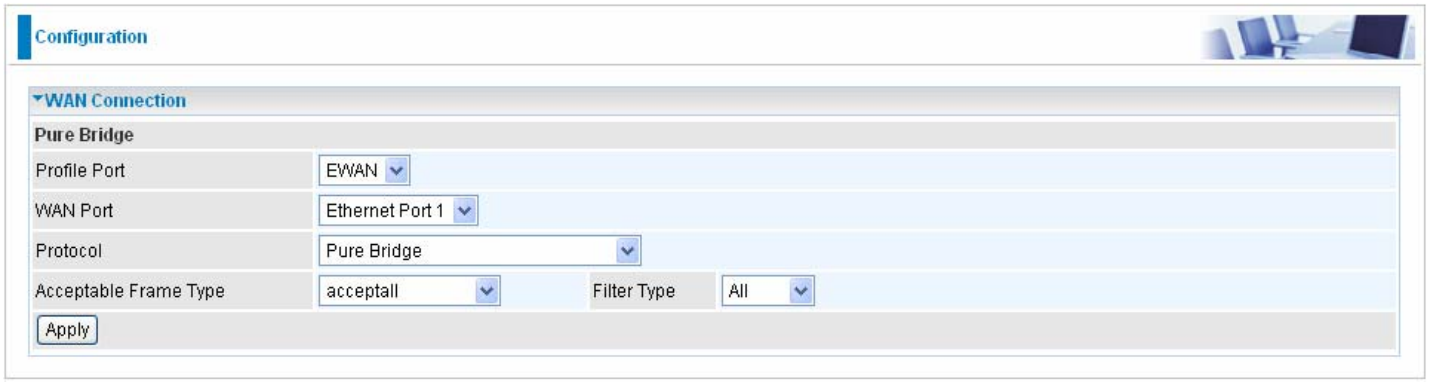
IPv6: check to enable IPv6 service. Enter IPv6 Gateway address and set IPv6 DNS as same in IPv4 mode.



IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ” ::” means to obtain IPv6 address automatically.

Obtain IPv6 DNS: check **Automatic** to obtain DNS automatically. If not, please type the concrete one in the Primary field.

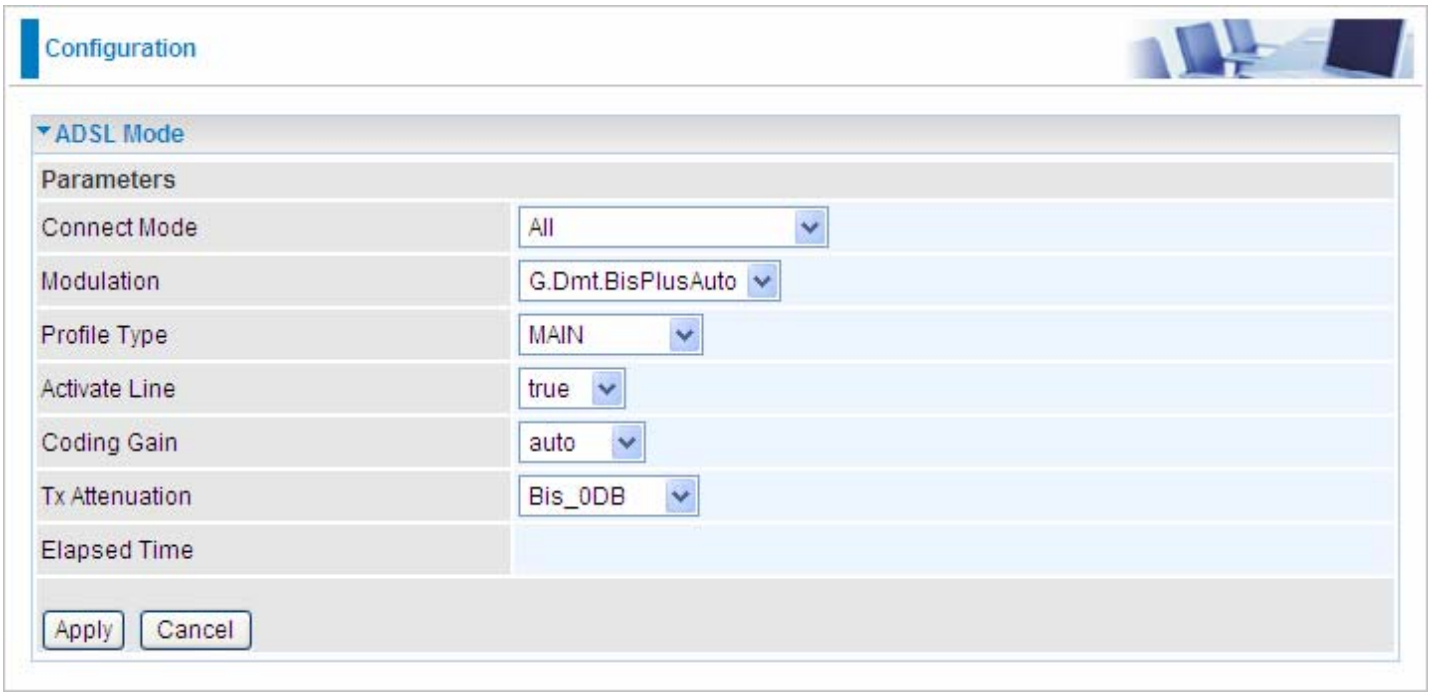
4. Pure Bridge: Select this item if just want to connect your ISP by other device or PC.



Acceptable Frame Type: Select accept all or accept tagged only. Accept all is default value.

Filter Type: Allow All, IP or PPPoE packets to go through the device.

ADSL Mode



Connect Mode: This mode will automatically detect your ADSL line code, ADSL2+, ADSL2, AnnexM2 and AnnexM2+, ADSL, All. Please keep it as the factory setting unless ADSL is detected as the symptom of synchronization problem.

Modulation: It will automatically detect the capability of your ADSL line mode. Please use the factory setting unless ADSL is detected as the symptom of synchronization problem.

Profile Type: Please keep the factory settings unless ADSL is detected as the symptom of low link rate or unstable problems. You may need to change the profile setting to reach the best ADSL line rate, it depends on the differences of DSLAM and location.

Activate Line: When set to false, the system will abort the ADSL line connection. When set to true, the system will reconnect the ADSL line.

Coding Gain: It reduces router's transmit power which will effect to router's downstream performance. Higher the gain will increase the downstream rate but it sometimes causes unstable ADSL line. The configurable ADSL coding gain is from 0 dB to 7dB, or automatic.

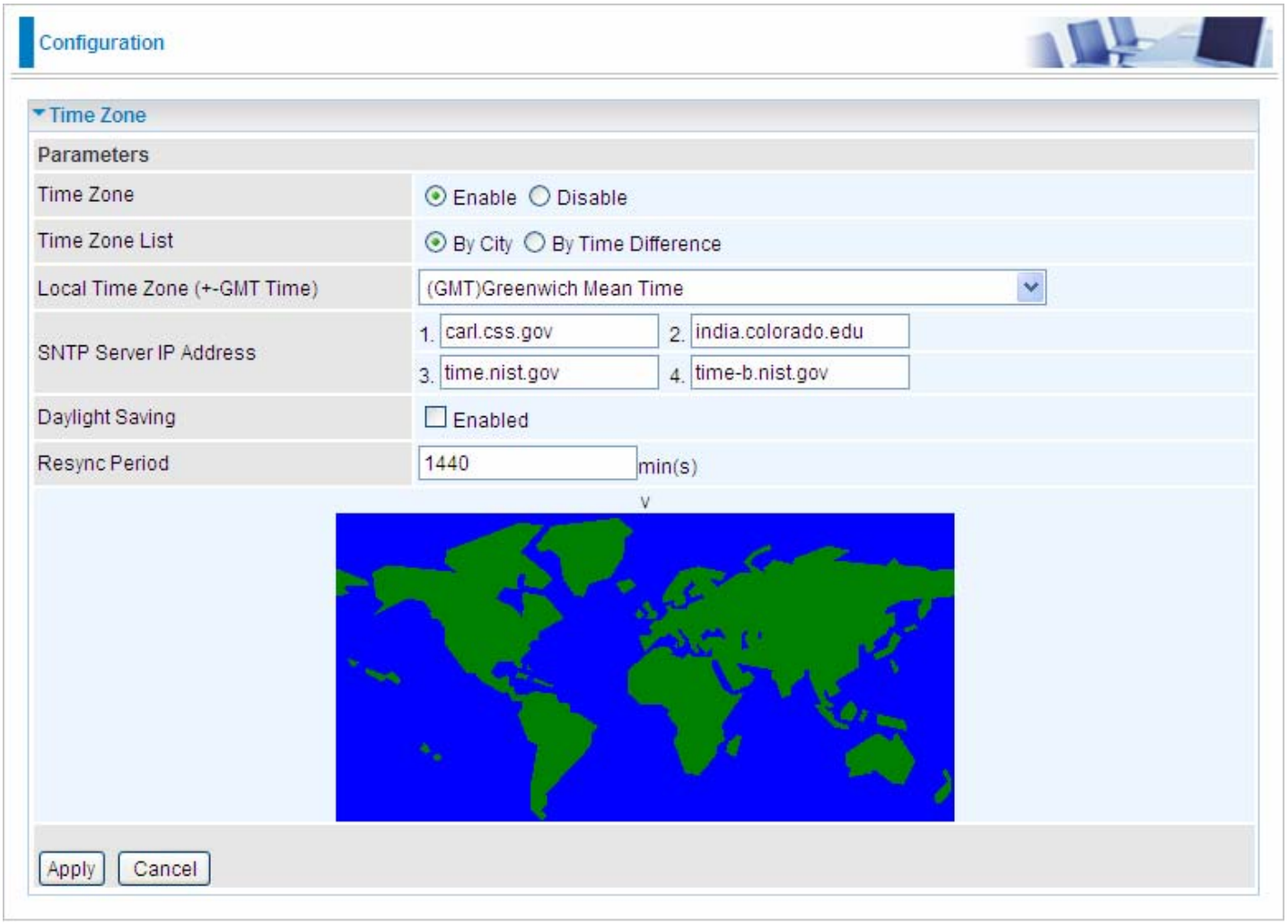
Tx Attenuation: It is the amount of power that modem (upstream) or DSLAM (downstream) is using. The lower the power the better the performance will be in modem upstream.

Elapsed Time: This is the ADSL connection uptime.

System

Here are the items within the System section: **Time Zone, Remote Access, Firmware Upgrade, Backup/Restore, Restart, User Management** and **Mail Alert.**

Time Zone

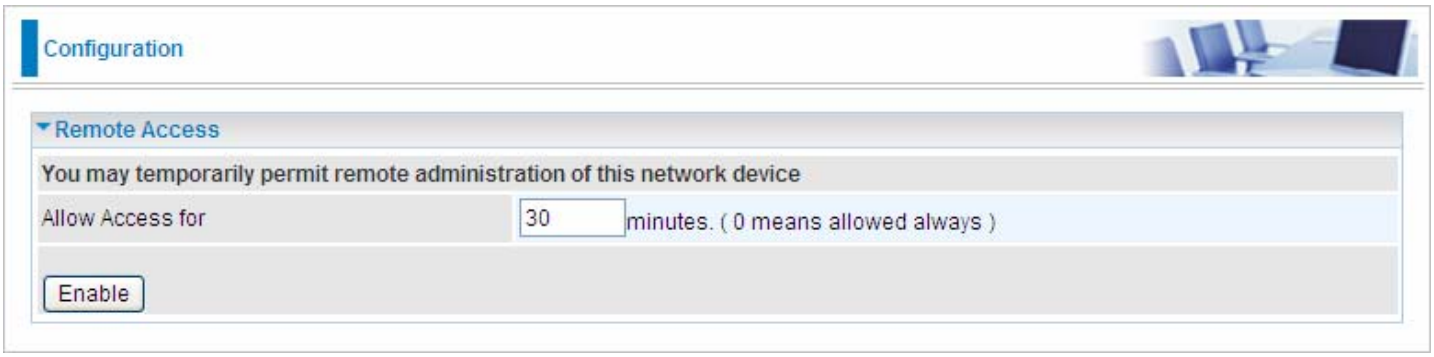


The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click Enable and click the Apply button. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Daylight Saving is also known as Summer Time Period. Many places in the world adapt it during summer time to move one hour of daylight from morning to the evening in local standard time. Check Enable checkbox to set your local time.

Resync Period (in minutes) is the periodic interval the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order to avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

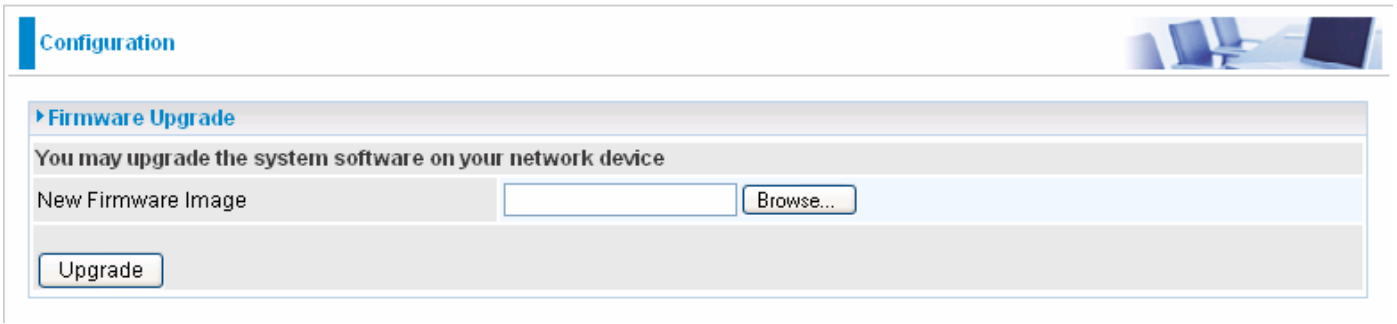
Remote Access



This feature enables system administrator to set the time interval where the router can be accessed for administration purpose from a remote site (i.e. from outside your LAN).

If you wish to permanently enable remote access, set the time period to 0 minute.

Firmware Upgrade

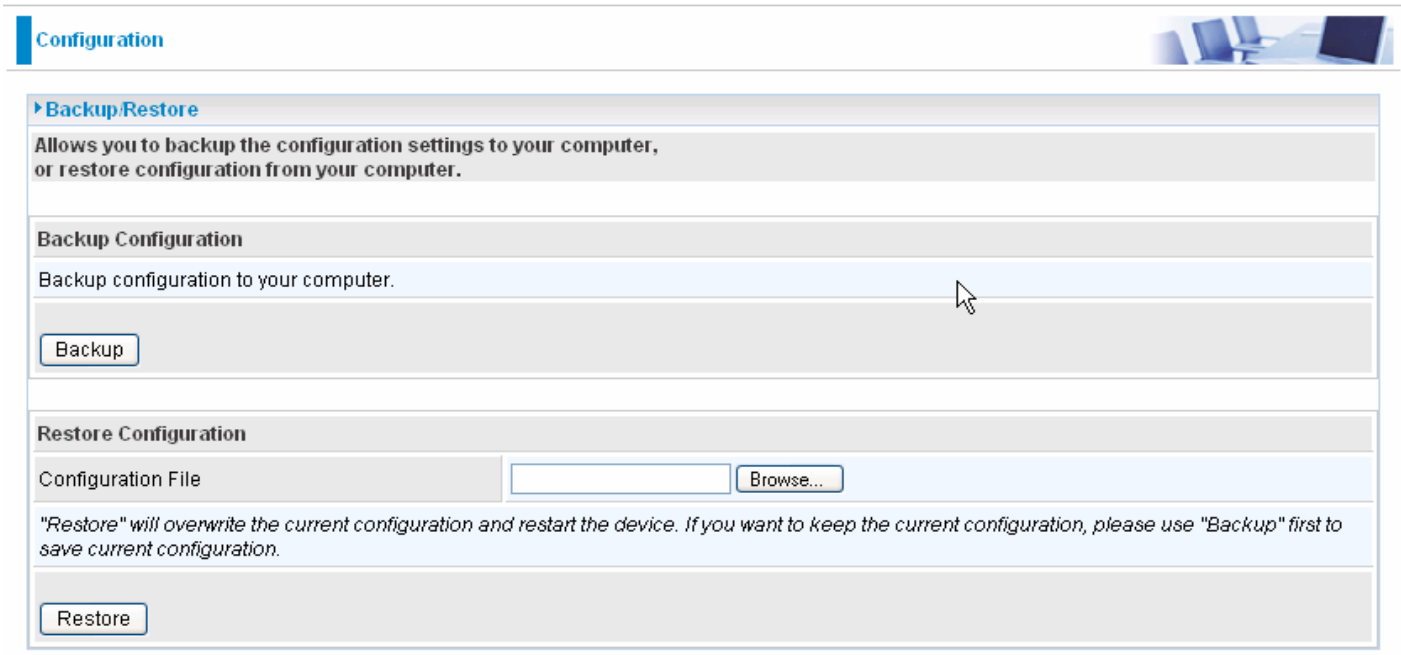


Your router firmware is the software that enables it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on Browse will allow you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

Backup / Restore


Configuration
Backup/Restore
Allows you to backup the configuration settings to your computer,
or restore configuration from your computer.
Backup Configuration
Backup configuration to your computer.
Backup
Restore Configuration
Configuration File
Browse...
"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.
Restore

This function allows you to save a backup of the current configuration of your router to a file on your PC, or to restore a previously saved configuration. This is very useful if you wish to customize the setting of the router, knowing in advance that you can always restore the setting if any mistakes do occur. Therefore, It is advisable that you create a backup of the configuration of your router before customizing its configuration.

Create a Router Configuration Backup

To create a backup of the setting, simply press the Backup button and specify the location on where to save your configuration file. You may also change the name of the file if you wish to keep multiple backups.

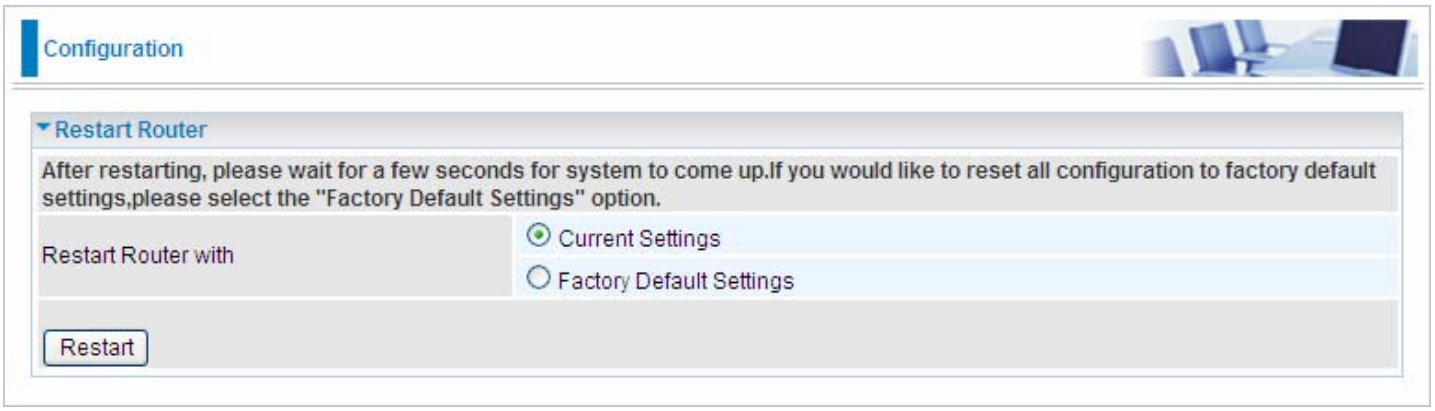
Restoring the Router Configuration

To restore the configuration of the router, press Browse to locate the configuration file from your PC. Once the file has been located, click on the file then click on the Restore button to load the setting.

Note: You should only restore the setting with the files that have been created using the Backup function with the most current firmware version. Settings files saved to your PC should not be manually edited in any way.

Restart Router

Click Restart with option Current Settings to reboot your router (and restore your last saved configuration).


Configuration
Restart Router
After restarting, please wait for a few seconds for system to come up.If you would like to reset all configuration to factory default settings,please select the "Factory Default Settings" option.
Restart Router with
Current Settings
Factory Default Settings
Restart

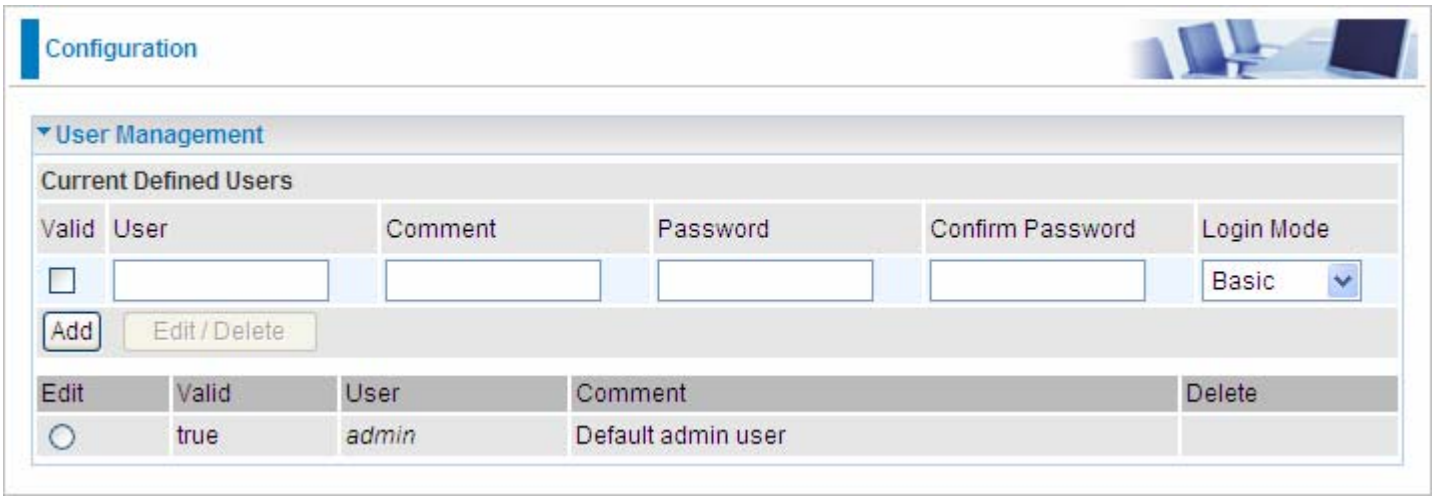
If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings.

You may also reset your router to factory settings by holding the small Reset pinhole button more than 6 seconds on the back of your router.

Caution: After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device again.

User Management

In order to prevent unauthorized access to your router's configuration interface, it requires that all users are to login the GUI with a password. You can set up multiple user accounts, each with their own password. You can Edit any existing user accounts and Add new user account to grant access to the device configuration interface.

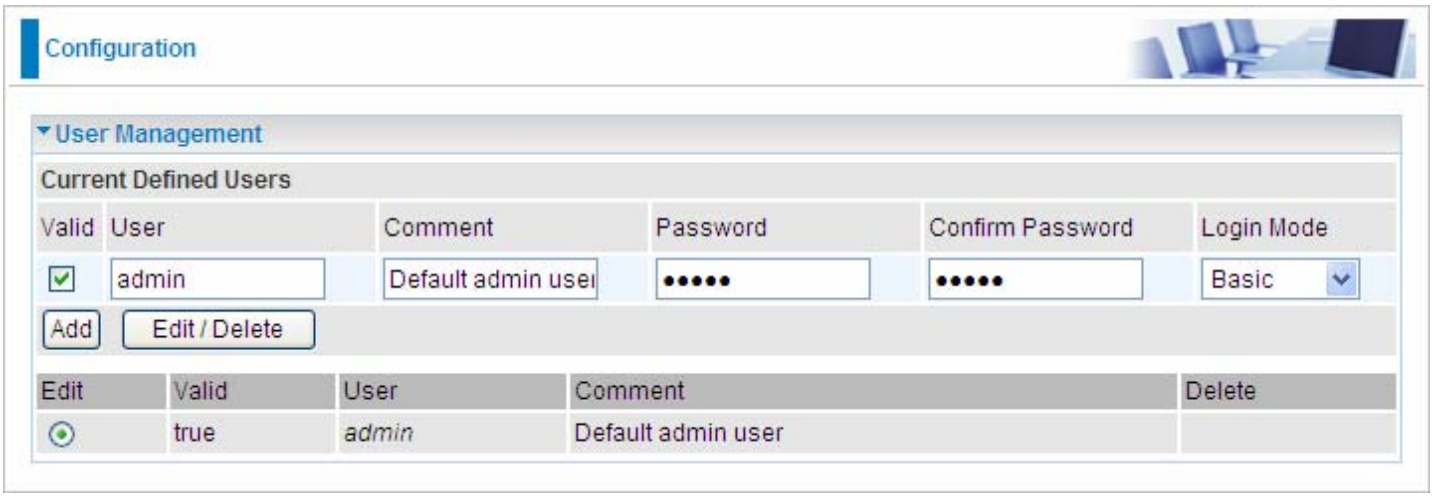


Edit Account Information

You can change the information of any account whether the account is active or valid.

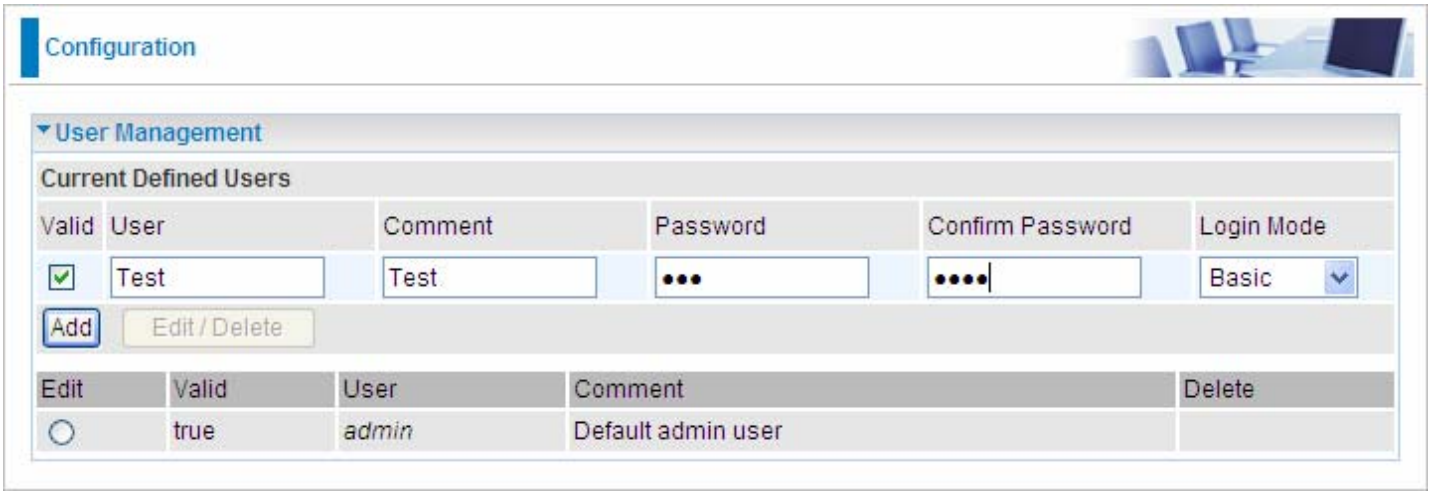
1. To edit an account, select the Edit radio button of the account to be edited. Once selected, all information of that account will be displayed.
2. Delete the information to be edited and replace it with the new one.
3. When it is done, simply click on the Edit/ Delete button to save your changes.

Note: It is recommended that you change the password immediately to prevent security breach to your GUI.



To Add an Account

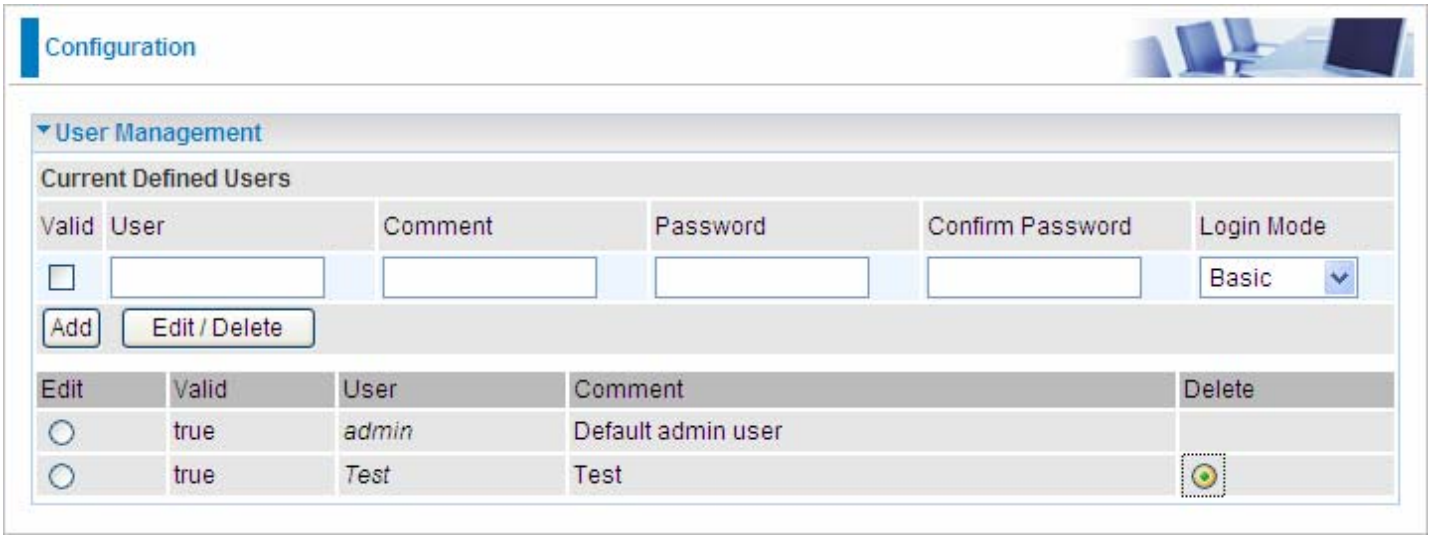
1. Check the Valid checkbox, fill in all the information: User name, Comment (optional), Password, Confirm Password.
2. When it is done, click the Add button.



To delete a user account:

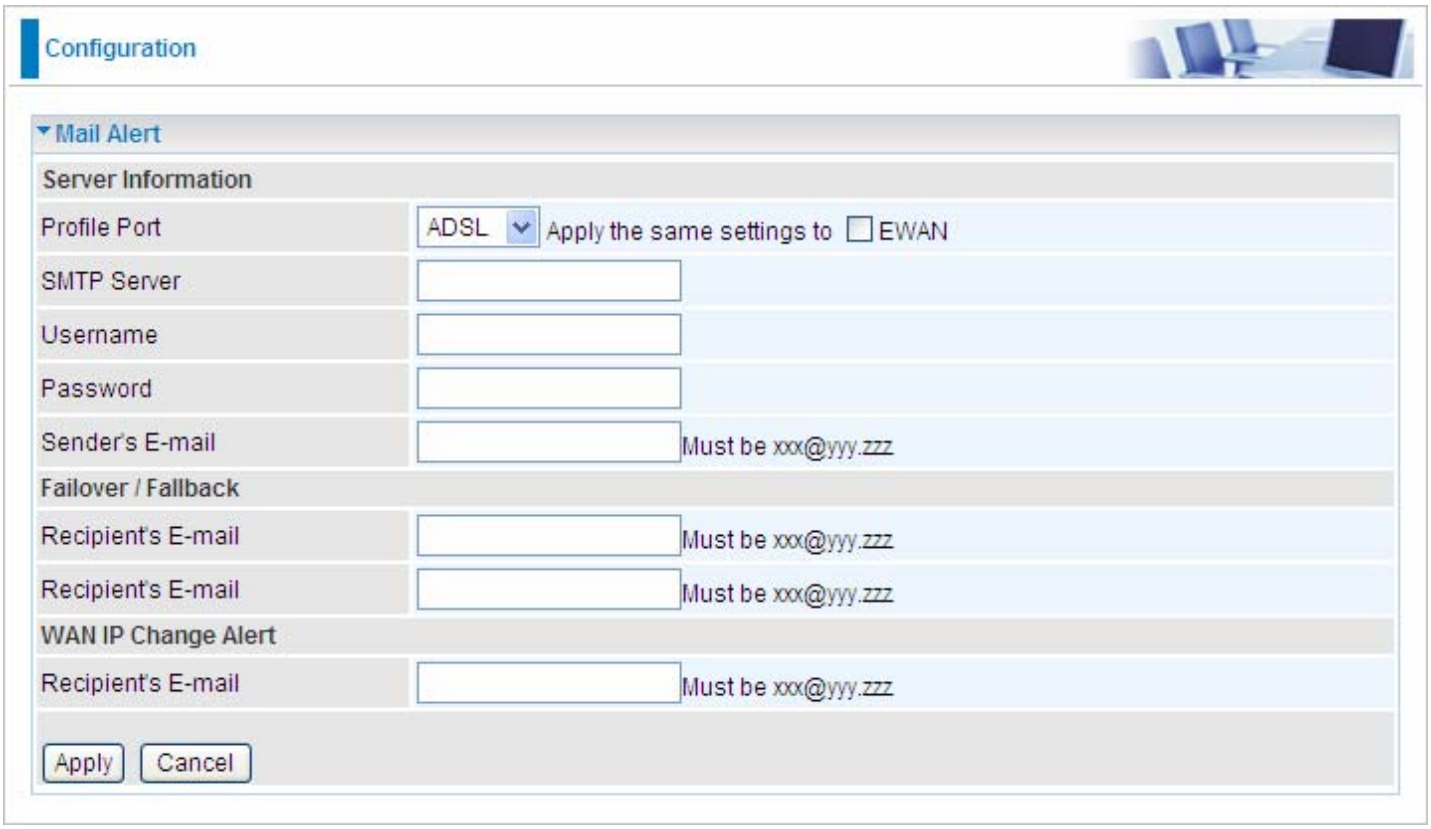
1. Click on the Delete radio button of the account you want to delete.
2. Then click the Edit/Delete to confirm the deletion.

Note: You can delete any user account except for the default admin account. Thus there is no delete radio button available for this account.



Mail Alert

Mail alert is designed to keep system administrator or other relevant personnel alerted of any unexpected events that might have occured to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.



SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

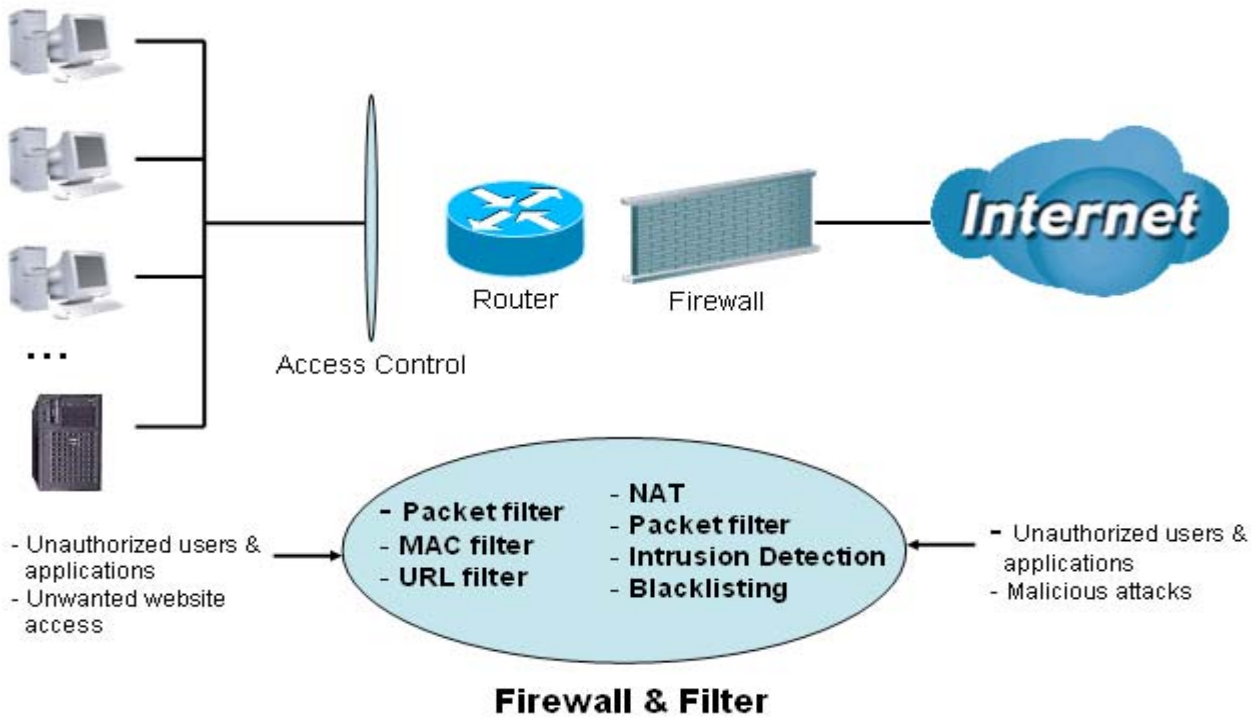
Sender's Email: Enter your email address.

Recipient's Email (Failover / Failback): Enter the email address that will receive the alert message once a computer / network server failover occurs.

Recipient's Email (WAN IP Change Alert): Enter the email address that will receive the alert message once a WAN IP change has been detected.

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for Internet access controlling from your LAN. This feature also protects your system from being attacked by hackers. When using NAT, the router acts as a "natural" Internet firewall, as all PCs on your LAN will have their own private IP addresses which are not directly accessible from the Internet. The router provides three levels of security support.



Firewall & Filter

NAT natural firewall: This masks LAN users' IP addresses which are invisible to users on the Internet, thus making it more difficult for a hacker to target a machine on your network. This natural firewall is turned on when NAT function is enabled.

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules to prevent unauthorized computers or applications to access your local network from the Internet.

Intrusion Detection: Enable Intrusion Detection to detect, prevent and log malicious attacks.

Access Control: Prevent access from PCs on your local network:

Firewall Security and Policy (General Settings): Outbound direction of Packet Filter rules to prevent unauthorized computers or applications from accessing the Internet.

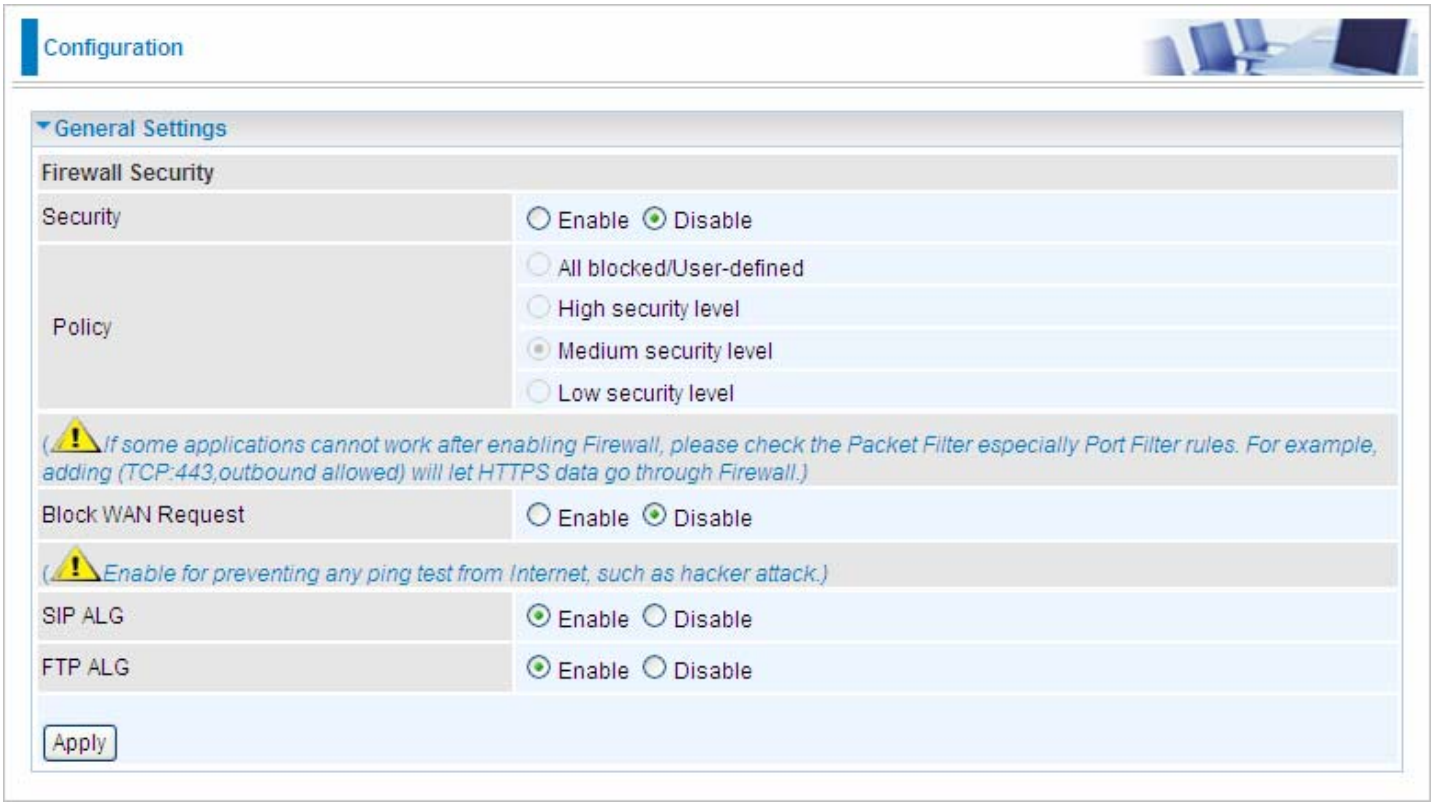
URL Filter: To block PCs on your local network from unwanted websites.

> **NOTE:** When using Virtual Server, your PC will thus become exposed in a certain degree to unknown users if specific ports are set to open in the firewall packet filter setting. The degree of exposure depends on the parameter set in the Virtual Server Setting.

Listed are the items under the Firewall section: **General Settings, Packet Filter, Intrusion Detection, URL Filter, IM/P2P Blocking** and **Firewall Log.**

General Settings

You can choose to disable Firewall and still be able to access the URL Filter, Intrusion Detection and IM/P2P Blocking or enable the Firewall using the preset filter rules and modify the port filter rules as required. The Packet Filter is used to filter packets based on Applications (Port) or IP addresses.



There are four policy options to choose from:

All blocked/User-defined: no predefined port or address filter rules by default, meaning that all inbound (Internet to LAN) and outbound (LAN to Internet) packets will be blocked. Users have to add their own filter rules to access the Internet.

High/Medium/Low security level: the predefined port filter rules for High, Medium and Low security are displayed in the Port Filters of the Packet Filter.

Select either High, Medium or Low security level to enable Firewall protection. The only difference between these three is the preset port filter rules in the Packet Filter. Firewall function is the same for all levels; it is only the list of preset port filters that changes between each setting. For more detail on level of preset port filter information, please refer to **Table 1: Predefined Port Filter**.

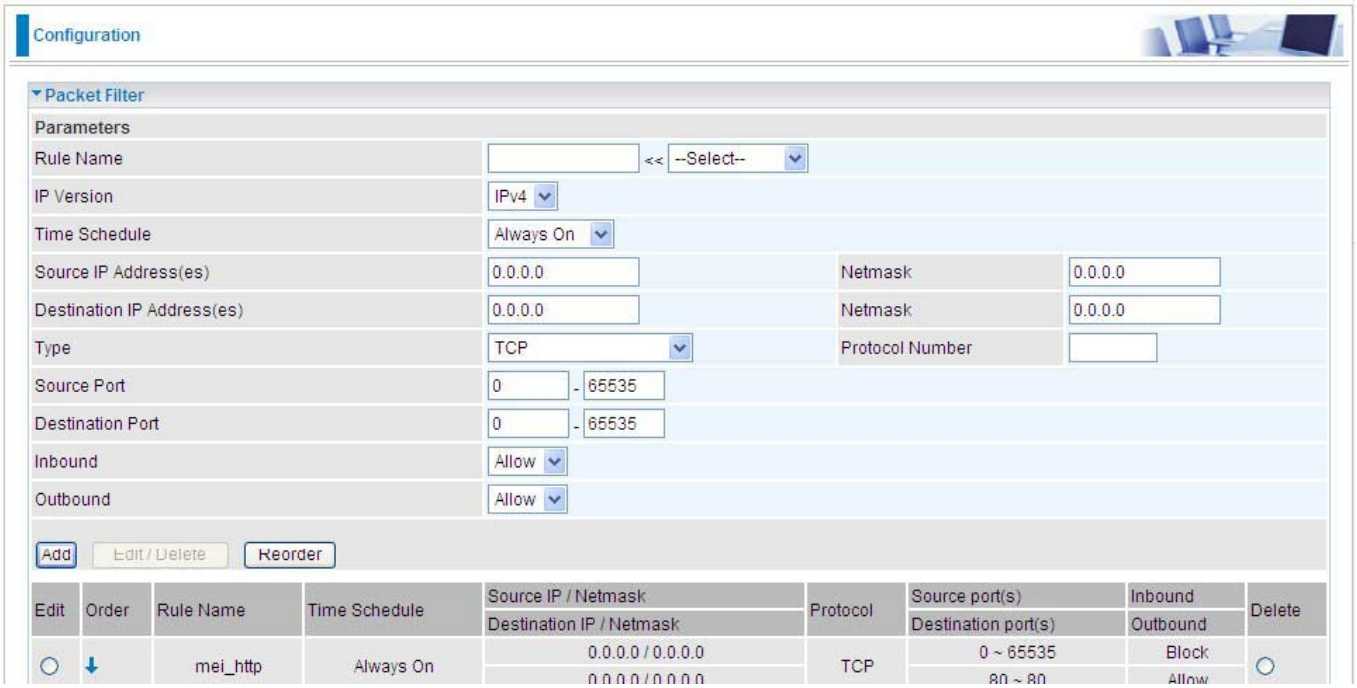
If you choose the preset security levels and add custom filters, the level of filter rules will be saved and you do not need to re-configure the rules again if you disable or switch to the other security level.

The “Block WAN Request” is a standalone function that is not affected by whether the security is enabled or disabled. This is used to prevent any scan tools that might be from hackers.

Any remote user attempting to perform this action may result in blocking all accesses to configure and manage the device from the Internet.

Packet Filter

This function is only available when Firewall is enabled with one of the four security levels selected (All blocked, High, Medium and Low). The preset port filter rules in the Packet Filter must be modified accordingly to the level of security selected. See Table1: Predefined Port Filter for more detail information.



Example: Predefined Port Filters Rules

The predefined port filter rules for High, Medium and Low security levels are listed. See Table 1.

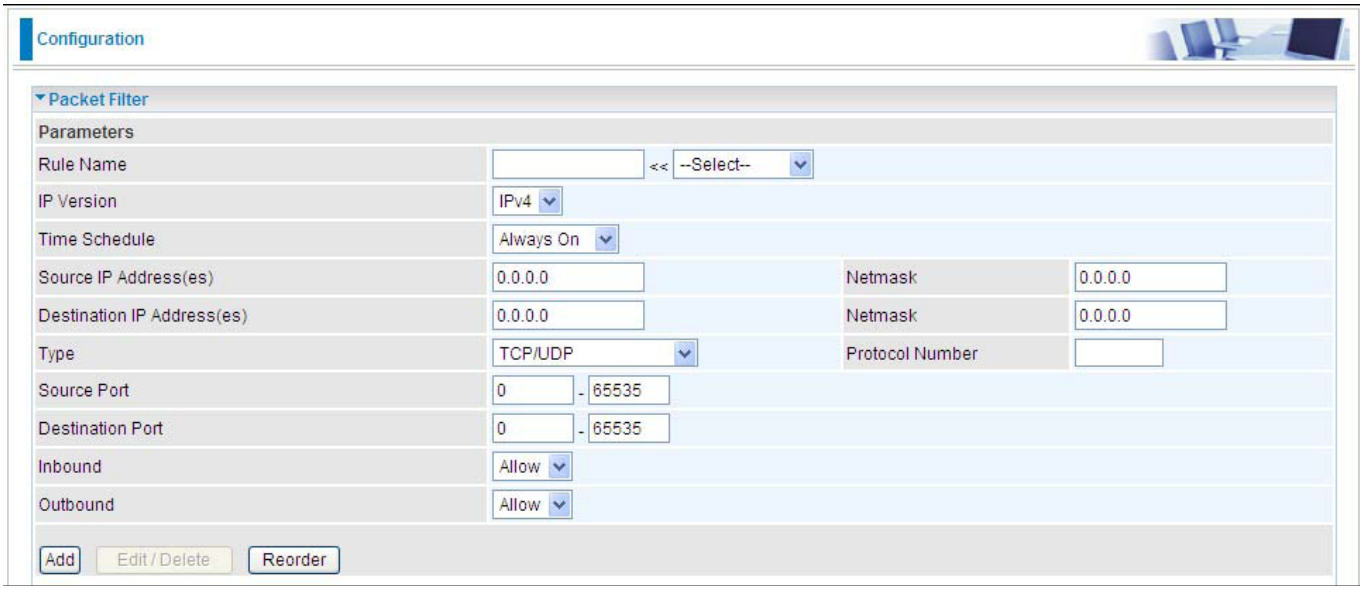
Note: Firewall – All Blocked/User-defined, you must define and create the port filter rules yourself. No predefined rule is being preconfigured.

Table 1: Predefined Port Filter

Application	Protocol	Port Number		Firewall - Low		Firewall - Medium		Firewall – High	
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS(53)	UDP	53	53	NO	YES	NO	YES	NO	YES
DNS(53)	TCP(6)	53	53	NO	YES	NO	YES	NO	YES
FTP(21)	TCP(6)	21	21	NO	YES	NO	YES	NO	NO
Telnet(23)	TCP(6)	23	23	NO	YES	NO	YES	NO	NO
SMPT(25)	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3(110)	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
NEWS(NNTP)	TCP(6)	119	119	NO	YES	NO	YES	NO	NO
PING	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	YES	YES	NO	YES	NO	NO
T.120(1503)	TCP(6)	1503	1503	YES	YES	NO	YES	NO	NO
SSH(22)	TCP(6)	22	22	NO	YES	NO	YES	NO	NO
NTP/SNTP	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTP/HTTP Proxy(8080)	TCP(6)	8080	8080	NO	YES	NO	NO	NO	NO
HTTPS(443)	TCP(6)	443	443	NO	YES	NO	YES	N/A	N/A
ICQ(5190)	TCP(6)	5190	5190	YES	YES	N/A	N/A	N/A	N/A
MSN(1863)	TCP(6)	1863	1863	YES	YES	N/A	N/A	N/A	N/A
MSN(7001)	UDP(17)	7001	7001	YES	YES	N/A	N/A	N/A	N/A
MSN VEDIO	TCP(6)	9000	9000	NO	YES	N/A	N/A	N/A	N/A

Inbound: Internet to LAN
Outbound: LAN to Internet
YES: Allowed
NO: Blocked
N/A: Not Applicable

Packet Filter – Add TCP/UDP Filter



Rule Name Helper: User defined description for entry identification. You may also choose from the Select drop-down menu for an existing predefined rule. The maximum name length is 32 characters.

Time Schedule: A self defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Source IP Address(es) / Destination IP Address(es): This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Select the Subnet Mask of the IP address range you wish to allow/block the traffic to or form. Set the IP address and Subnet Mask to 0.0.0.0 to inactive the Address-Filter rule.

Tip: To block access, to/from a single IP address, enter that IP address as the Host IP Address and use a Host Subnet Mask of "255.255.255.255".

Type: It is the packet protocol type used by the application, select TCP, UDP or both TCP/UDP.

Protocol Number: Insert the port number.

Source Port: This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range 0 ~ 65535. It is recommended that this option be configured by an advanced user.

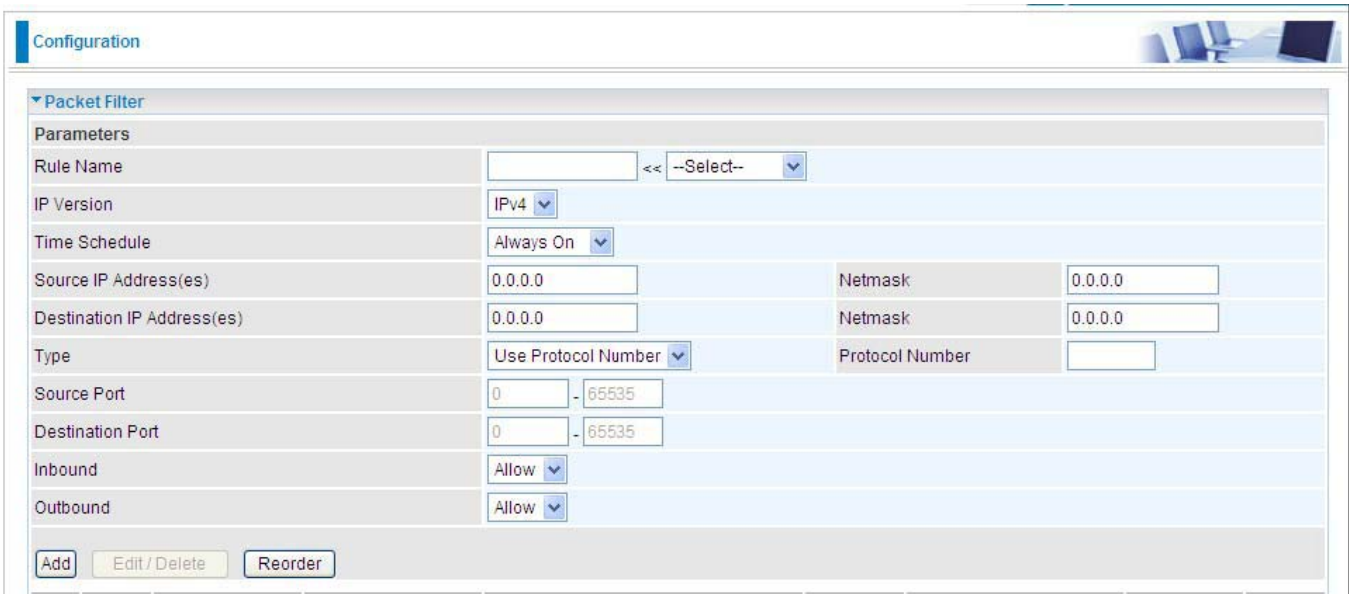
Destination Port: This is the Port or Port Ranges that defines the application.

Inbound / Outbound: Select Allow or Block the access to the Internet ("Outbound") or from the Internet ("Inbound").

When all changes is made, click Add button to apply your changes.

Packet Filter – Add Raw IP Filter

Go to “Type” drop-down menu, select “Use Protocol Number”.



Rule Name Helper: User defined description for entry identification. You may also choose from the Select drop-down menu for an existing predefined rule.

Time Schedule: A self defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Source IP Address(es) / Destination IP Address(es): This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Select the Subnet Mask of the IP address range you wish to allow/block the traffic to or form; set IP address and Subnet Mask to 0.0.0.0 to inactive the Address-Filter rule.

Tip: To block access to/from a single IP address, enter that IP address as the Host IP Address and use a Host Subnet Mask of “255.255.255.255”.

Type: It is the packet protocol type used by the application, select TCP, UDP or both TCP/UDP.

Protocol Number: Insert the port number, i.e. GRE 47.

Source Port: This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range 0 ~ 65535. It is recommended that this option be configured by an advanced user.

Destination Port: This is the Port or Port Ranges that defines the application.

Inbound / Outbound: Select Allow or Block the access to the Internet (“Outbound”) or from the Internet (“Inbound”).

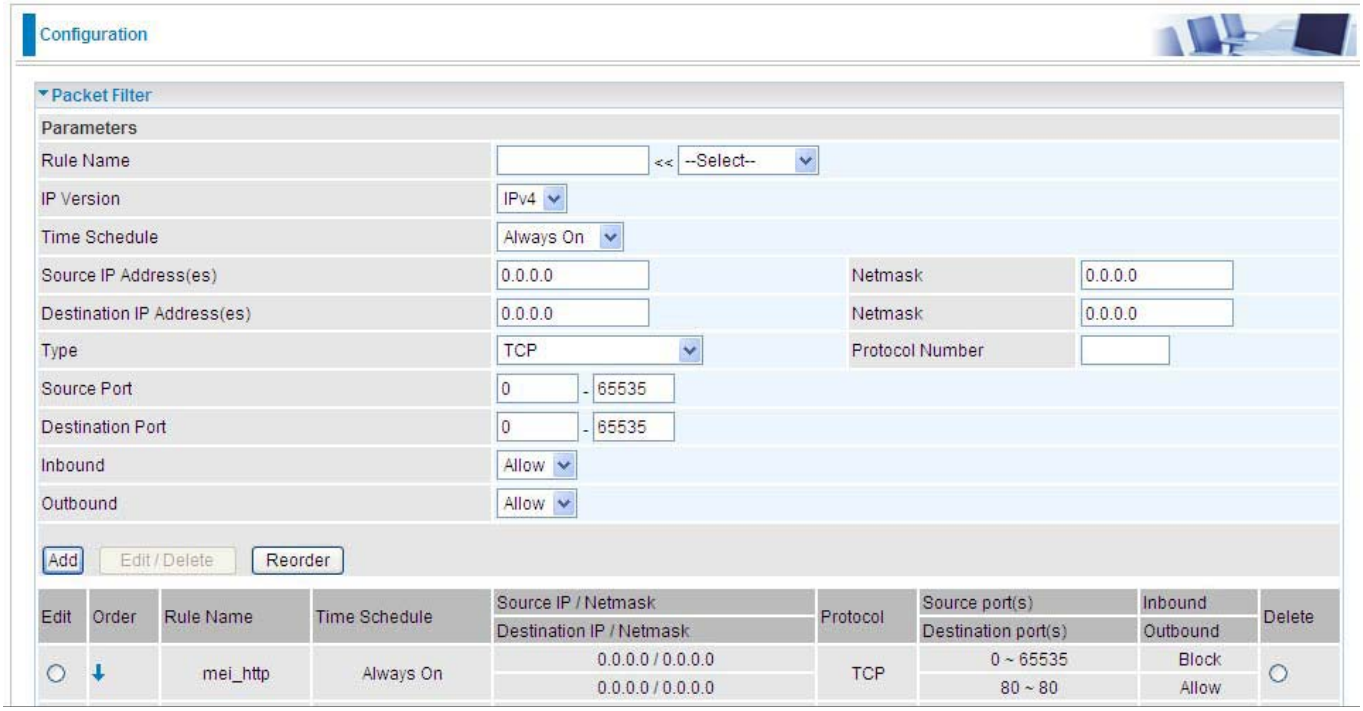
When all changes is made, click Add button to apply your changes.

Example: Configuring your firewall to allow a publicly accessible web server on your LAN

The predefined port filter rule for HTTP (TCP port 80) is the same whether the firewall is set to a high, medium or low security level. To setup a web server located on the local network when the firewall is enabled, you have to configure the Port Filters setting for HTTP.

As you can see from the diagram below, when the firewall is enabled with one of the three presets (Low/Medium/High) security level selected, an inbound HTTP access is not allowed which means remote access through HTTP to your router is not allowed.

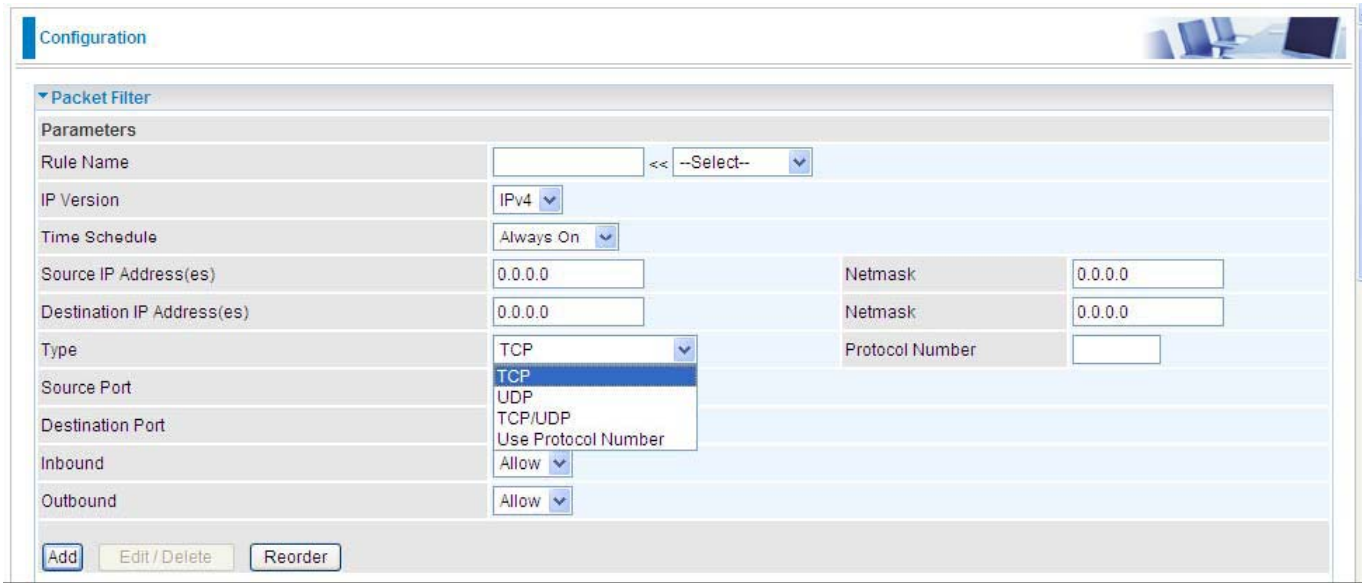
Note: Inbound indicates accessing from the Internet to LAN and Outbound is from LAN to the Internet.



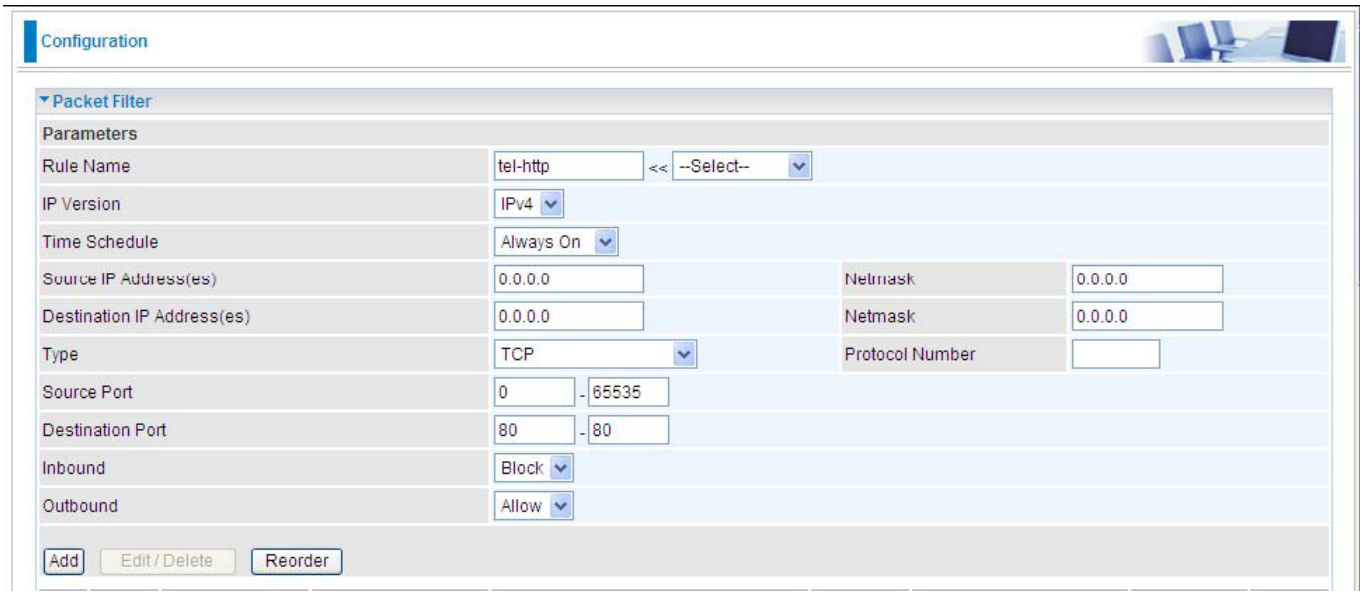
Configuring Packet Filter:

1. Click Packet Filters. You will then be presented with the predefined port filter rules screen (in this case for the low security level), shown below:

Note: You may click Edit the predefined rule instead of Delete it. This is an example to show to how you add a filter on your own.

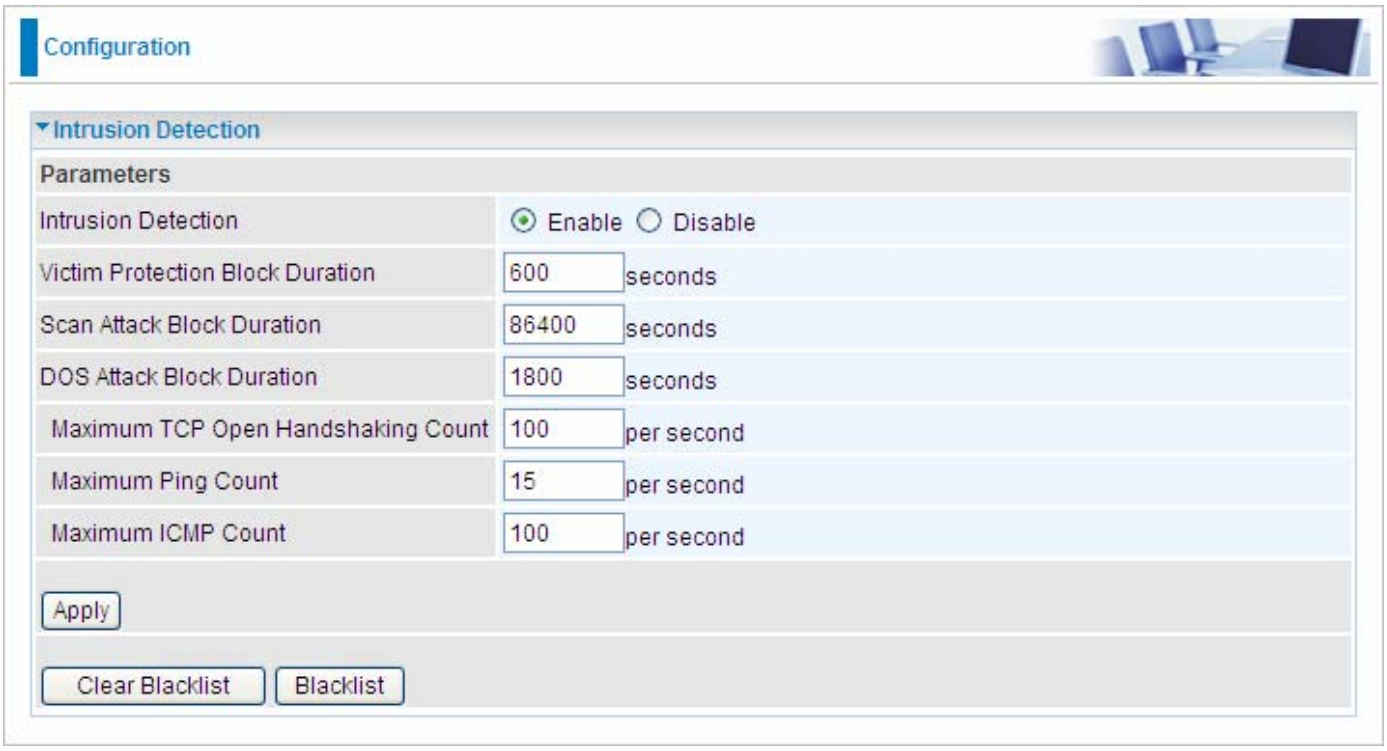


2. If you want to delete a filter rule, select the delete radio button of the HTTP rule you want to delete. Then click the Edit/Delete button to delete the rule.



3. To add a new rule, Input the Rule Name, Time Schedule, Source/Destination IP, Type, Source/ Destination Port, Inbound and Outbound. Then click the Add button.

Intrusion Detection



The router Intrusion Detection System (IDS) is used to detect hacker's attack and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.

Blacklist: If the router detects a possible attack, the source IP or destination IP address will be added to the Blacklist. Any further attempts using this IP address will be blocked for the time period specified in the Block Duration. The default setting for this function is false (disabled). Some types of attack are denied immediately without using the Blacklist function, such as Land attack and Echo/CharGen scan.

Intrusion Detection: If enabled, IDS will block Smurf attack attempts. Default is false.

Block Duration:

Victim Protection Block Duration: This is the duration for blocking *Smurf* attacks. Default value is 600 seconds.

Scan Attack Block Duration: This is the duration for blocking hosts that attempt a possible Scan attack. Scan attack types include *X'mas scan, IMAP SYN/FIN scan* and similar attempts. Default value is 86400 seconds.

DoS Attack Block Duration: This is the duration for blocking hosts that attempt a possible Denial of Service (DoS) attack. Possible DoS attacks this attempts to block include *Ascend Kill* and *WinNuke*. Default value is 1800 seconds.

Max TCP Open Handshaking Count: This is a threshold value to decide whether a *SYN Flood* attempt is occurring or not. Default value is 100 TCP SYN per seconds.

Max PING Count: This is a threshold value to decide whether an *ICMP Echo Storm* is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Max ICMP Count: This is a threshold to decide whether an *ICMP flood* is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

Clear Blacklist: Clear the current blacklist.

Blacklist: Show the blacklist information.

For SYN Flood, ICMP Echo Storm and ICMP flood, IDS will just warn the user in the Event Log. It cannot protect against such attacks.

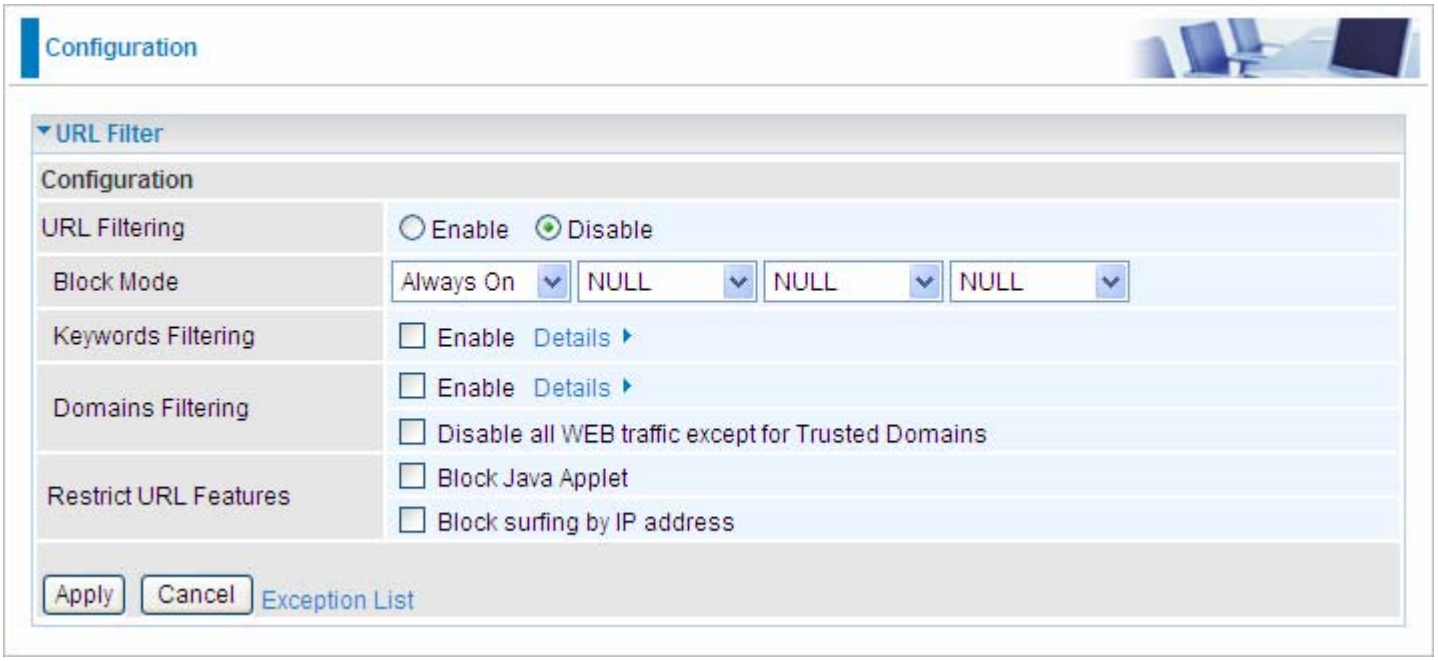
Table 2: Hacker attack types recognized by the IDS

Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP
Src Port: Source Port
Dst Port: Destination Port
Dst IP: Destination IP

URL Filter

URL (Uniform Resource Locator) (e.g. an address in the form of http://www.abcde.com or http://www.example.com) filter rule allows you to prevent users on your network from accessing specific websites defined by their URL. There are no predefined URL filter rules, therefore you can add filter rules to meet your requirements.



Enable/Disable: To enable or disable URL Filter feature.

Block Mode: It can support up to 4 timeslots.

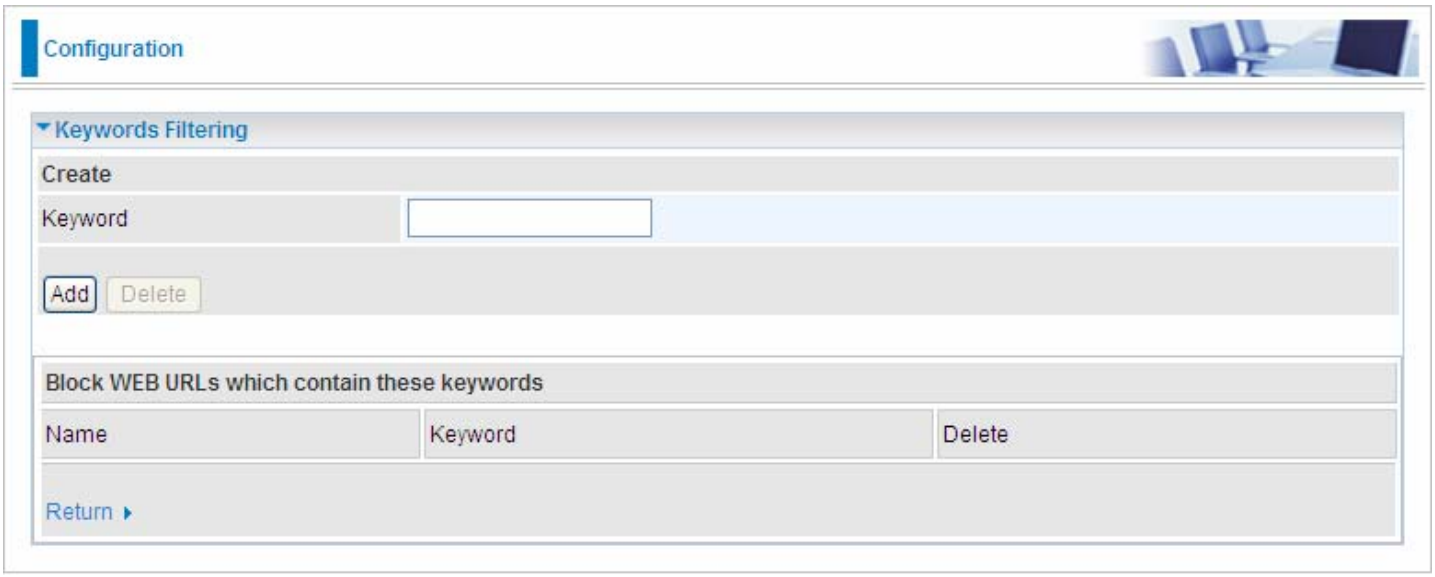
- **Disabled:** No action will be performed by the Block Mode.

- **Always On:** Action is enabled. URL filter rules will be monitoring and checking all hours of the day.

- **TimeSlot1 ~ TimeSlot16:** It is self-defined time period. You may specify the time period to check the URL filter rules, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

Keywords Filtering: Allow blocking against specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

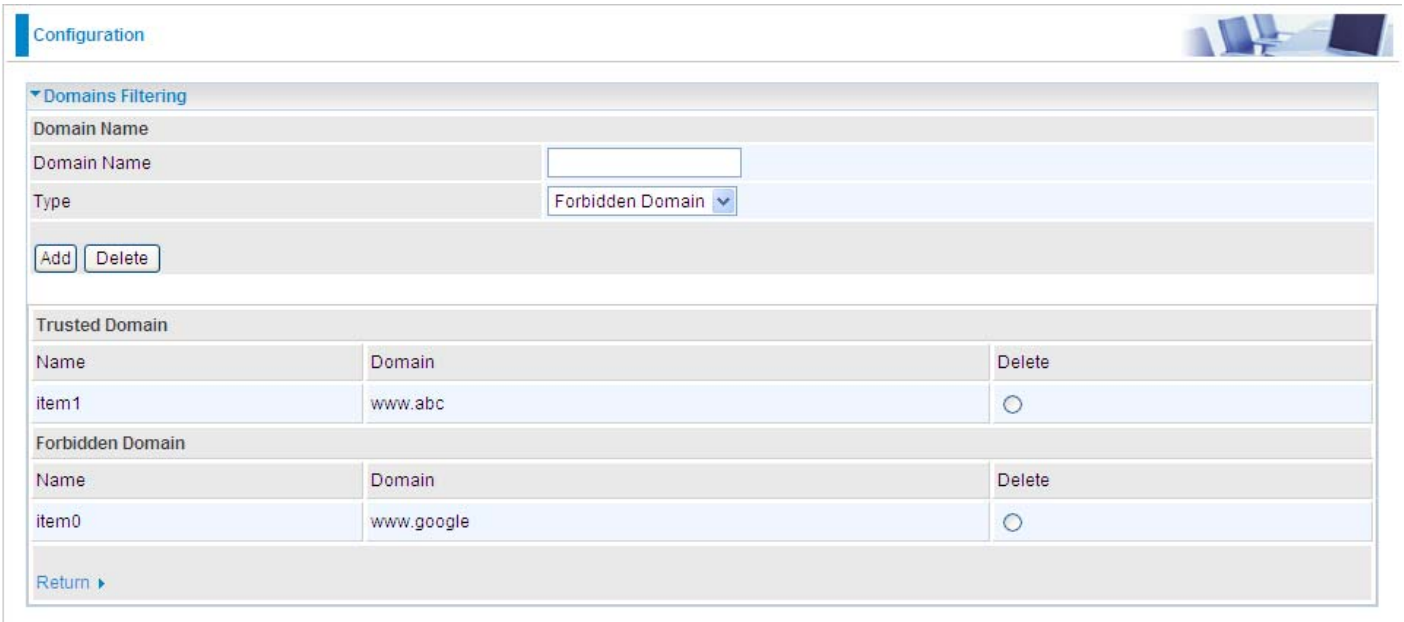
For example, if the URL is http://www.abc.com/abcde.html, the connection will be dropped if the keyword "abcde" occurs in the URL.



Domains Filtering: This function checks the whole URL address but not the IP address against your list of domains to block or allow. If it is matched, the URL request will either be sent (Trusted) or dropped (Forbidden). For this function to be activated, both enable and disable checkboxes of Domain Filtering must be checked. Here is the checking procedure:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, check if it is listed in the forbidden list. If yes, then the connection attempt will be dropped.
3. If the packet does not match either of the above two conditions, it is sent to the remote web server.
4. Please be noted that the completed URL, "www" + domain name should be specific. e.g.: In order to block traffic to **www.google.com.au**, enter "**www.google**" or "**www.google.com**"

In the example below, the URL request for **www.abc.com** will be sent to the remote web server because it is listed in the trusted list, whilst the URL request for **www.google** or **www.google.com** will be dropped, because **www.google** is in the forbidden list.



Example:

Andy wishes to disable all WEB traffic except for the ones listed in the trusted domain, which would prevent Bobby from accessing other websites. Andy selects both conditions in the Domain Filtering thinking that this will stop Bobby. But Bobby knows this function, Domain Filtering, ONLY disables all WEB traffic except for Trusted Domain, BUT not its IP address. If this is the situation, Block surfing by IP address function can become helpful. Now, Andy can successfully prevent Bobby from accessing other websites.

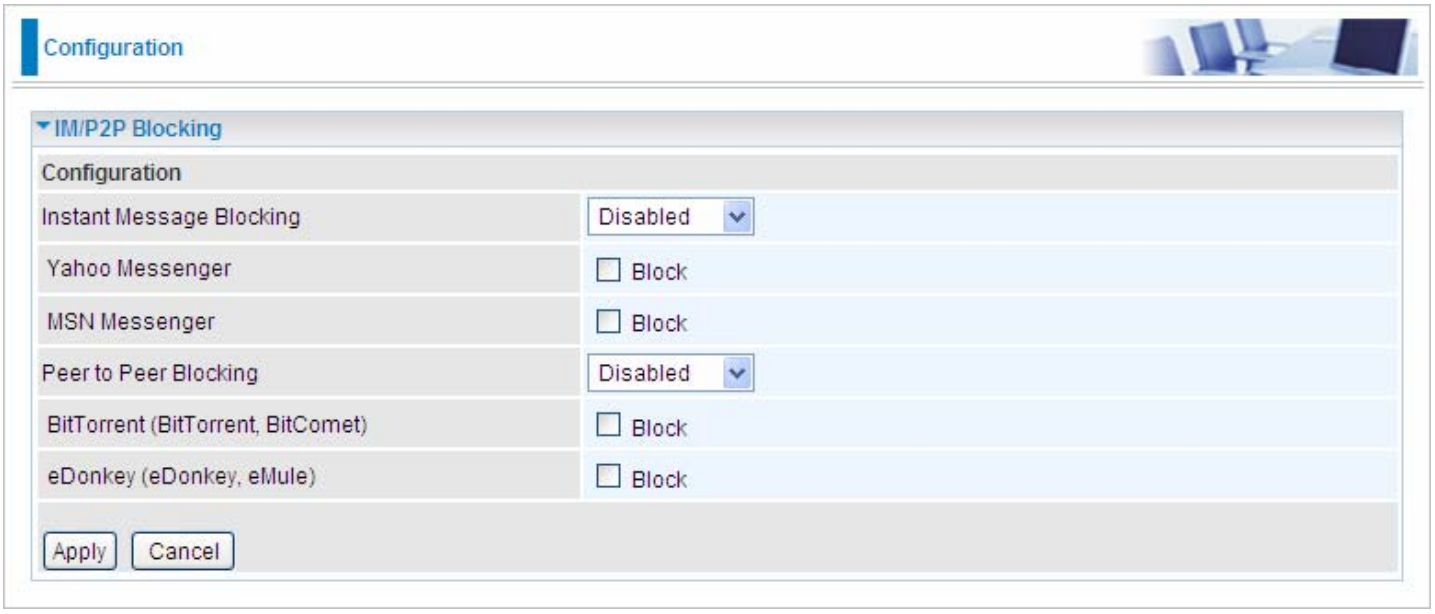
Restrict URL Features: This function enhances the restriction to your URL rules.

Block Java Applet: This function can block Web content that includes Java Applets. It is to prevent someone who wants to damage your system via standard HTTP protocol.

Block surfing by IP address: A further restriction against someone who uses IP address as URL to cheat around the Domains Filtering rule. Activates only if Domain Filtering is enabled.

IM / P2P Blocking

IM, short for Instant Message, is a client software that allows users to communicate & exchange text messages with other IM users in real time over the Internet. A P2P application, known as Peer-to-peer, is group of users who share their files with each other within the network over the Internet across the globe. Both Instant Message and Peer-to-peer applications make communication faster and easier but your network can become increasingly insecure at the same time. Billion's IM and P2P blocking helps users to restrict LAN PCs to access the commonly used IM, Yahoo and MSN, and P2P, BitTorrent and eDonkey, applications over the Internet.



Instant Message Blocking: The default is set to Disabled.

Disabled: Instant Message blocking is not triggered. No action will be performed.

Always On: Action is enabled.

TimeSlot1 ~ TimeSlot16: This is the self defined time period. You may specify the time period to trigger the blocking, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

Yahoo/MSN Messenger: Check the checkbox to block either or both Yahoo or/and MSN Messenger. To be sure you enabled the *Instant Message Blocking* first.

Peer to Peer Blocking: The default is set to Disabled.

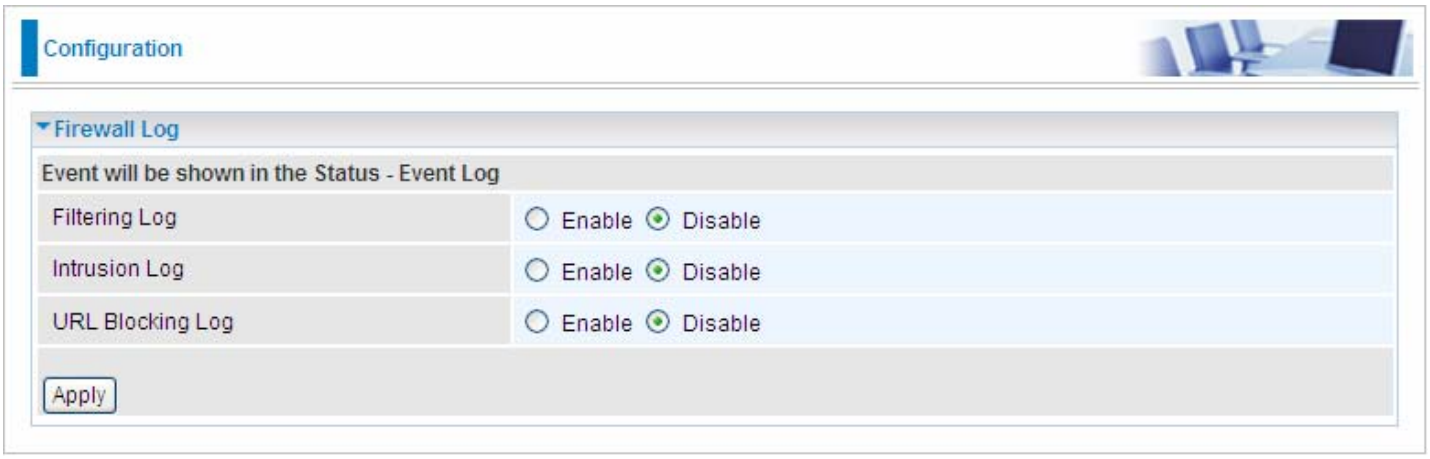
Disabled: Instant Message blocking is not triggered. No action will be performed.

Always On: Action is enabled.

TimeSlot1 ~ TimeSlot16: This is the self defined time period. You may specify the time period to trigger the blocking, i.e. during working hours. For setup and detail, refer to Time Schedule section.

BitTorrent / eDonkey: Check the checkbox to block either or both Bit Torrent or/and eDonkey. To be sure you enabled the Peer to Peer Blocking first.

Firewall Log



Firewall Log displays a log that contains information of any unexpected actions that occur to your firewall settings.

Check the Enable checkbox to activate event logging.

Log information can be seen in the Status – Event Log after the feature is enabled

VoIP - Voice over Internet Protocol

VoIP enables telephone calls through existing Internet connection instead of going through the PSTN (Public Switched Telephone Network). It is not only cost-effective, especially for a long distance telephone charges, but also toll-quality voice calls over the Internet.

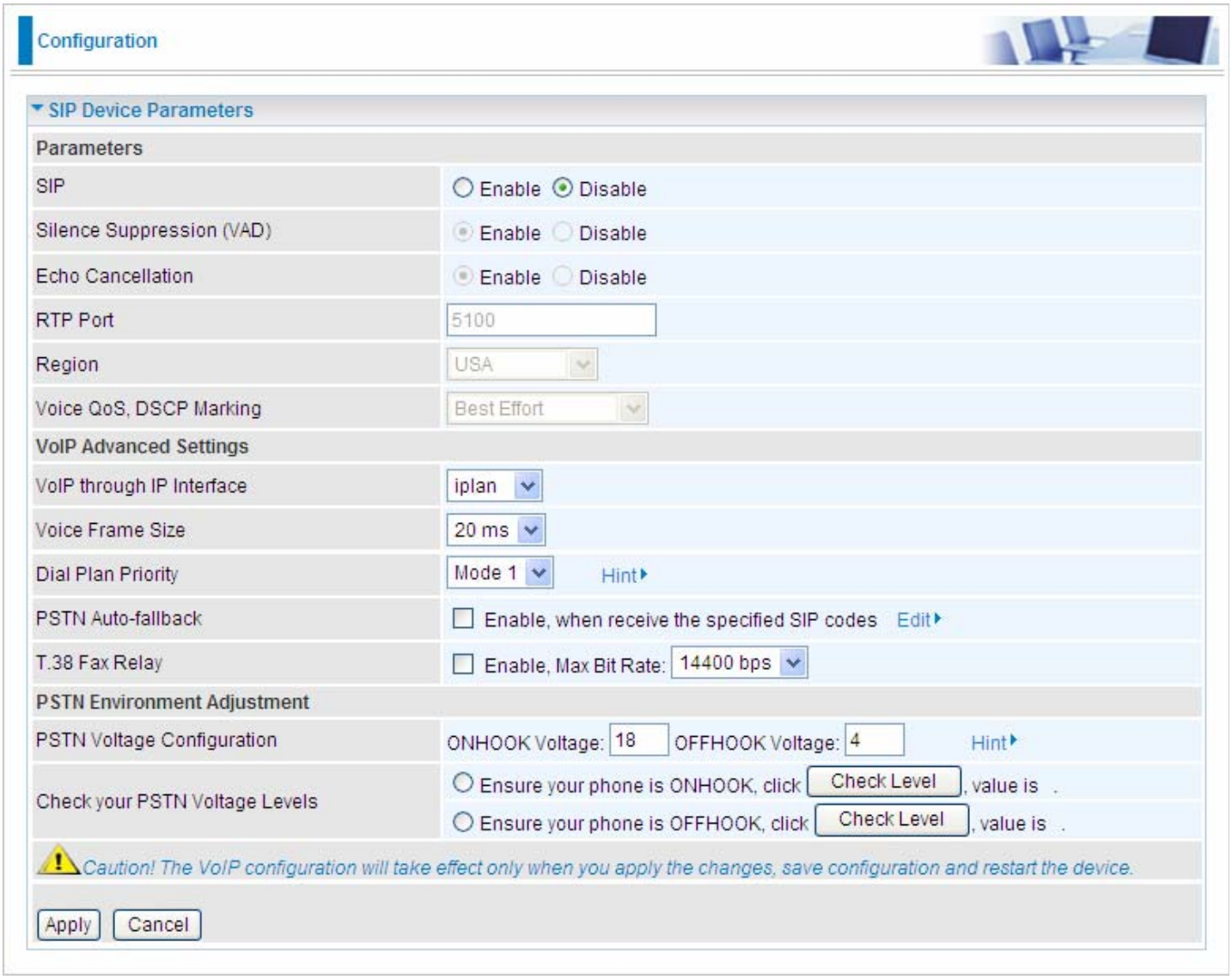
Attention

After completing VoIP configuration, remember to apply the changes. SAVE CONFIG and restart to activate your VoIP.

Here are the items within the VoIP section: **SIP Device Parameters, SIP Accounts, Phone Port, PSTN Dial Plan, VoIP Dial Plan, Call Features, Speed Dial** and **Ring &Tone.**

SIP Device Parameters

This section provides easy setup for your VoIP service. Phone port 1 can be registered to different SIP Service Provider.



SIP Device Parameters

SIP: To use VoIP SIP as VoIP call signaling protocol. Default is set to Disable.

Silence Suppression (VAD): Voice Activation Detection (VAD) prevents transmitting the nature silence to consume the bandwidth. It is also known as Silence Suppression which is a software application that ensures the bandwidth is reserved only when voice activity is activated. Default is set to Enable.

Echo Cancellation: G.168 echo canceller is an ITU-T standard. It is used for isolating the echo while you are on the phone. This helps you not to hear much of your own voice reflecting on the phone while you talk. Default is set to Enable.

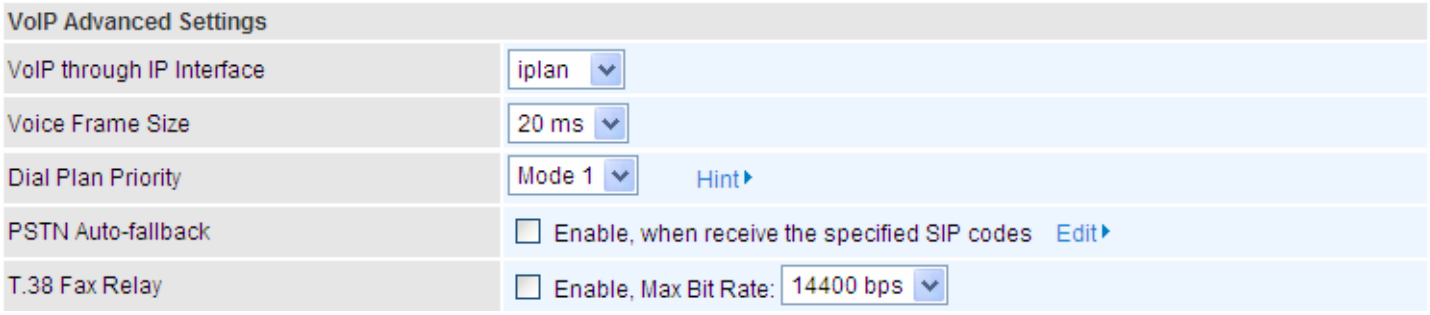
RTP Port: Provide the based value from the media (RTP) ports that are assigned for various endpoints and the different call sessions that may exist within an end-point. (Range from 5100 to 65535, default value is 5100)

Region: This selection is a drop-down box, which allows user to select the country for which the VoIP device must work. When a country is selected, the country parameters are automatically loaded.

Voice QoS, DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to assign specific application traffic to be executed in priority by the next Router based on the DSCP value. See Table 4. The DSCP Mapping Table:

Note: To be sure the router(s) in the backbones network have the capability in executing and checking the DSCP through-out the QoS network.

Advanced – Parameters



VoIP through IP Interface: IP Interface decides where to send/receive the voip traffic; it includes: ipwan and iplan. Easy way to select the interface is to check the location of the SIP server. If it locates some where in the Internet then select **ipwan.** If the VoIP SIP server is on the local Network then select **iplan.**

Voice Frame Size: Frame size is available from 10ms to 60ms. Frame size meaning how many milliseconds the Voice packets will be queued and sent out. It is ideal to have the same frame size in both of Caller and Receiver.

Dial Plan Priority: Define the priority between VoIP and PSTN dial plan.

PSTN Auto-fallback: Whenever VoIP SIP responses error and error code matching with the codes in the **Edit** section, the VoiP calls will automatically fallback to PSTN. In the other word, the call will be called via the PSTN when VoIP SIP returns an error code.

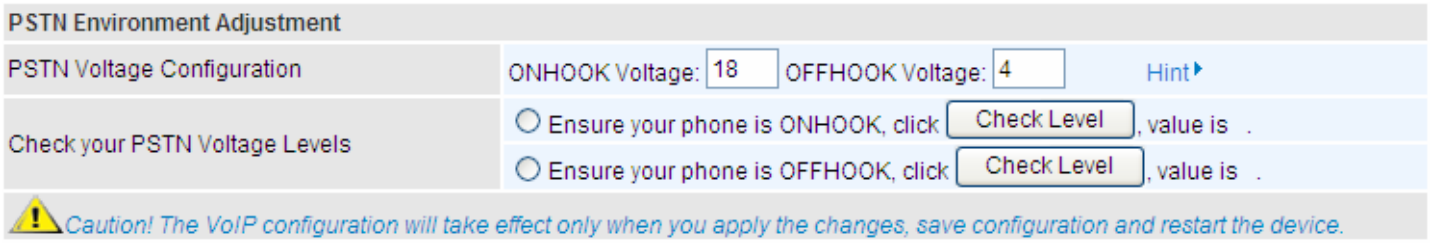
Click the **Edit** to add or remove the responses code. To be sure the code is separated by a comma (,).

For more information about SIP responses codes, please check Here to link to **http://voip-info.org/wiki/view/sip+response+codes** where you can get to know the meaning of each error code.

T.38 Fax Relay: It allows the transfer of facsimile documents in real-time between two standard Group 3 facsimile terminals over the Internet or other networks using IP protocols. It will only function when both sites are support this feature and enabled.

Advanced – PSTN Environment Adjustment

PSTN Environment Adjustment options will help you to adjust the onhook and offhook voltage detection values for your environment. You should use these if the default values are incorrect and result in PSTN calls not being detected properly, e.g. calls being terminated within 5 seconds of being answered. The actual levels are determined by your environment including the number and type of telephones used.


PSTN Environment Adjustment
PSTN Voltage Configuration
ONHOOK Voltage: 18
OFFHOOK Voltage: 4
Hint
Check your PSTN Voltage Levels
Ensure your phone is ONHOOK, click
Check Level
, value is .
Ensure your phone is OFFHOOK, click
Check Level
, value is .
Caution! The VoIP configuration will take effect only when you apply the changes, save configuration and restart the device.

Note: ONHOOK means hung up.

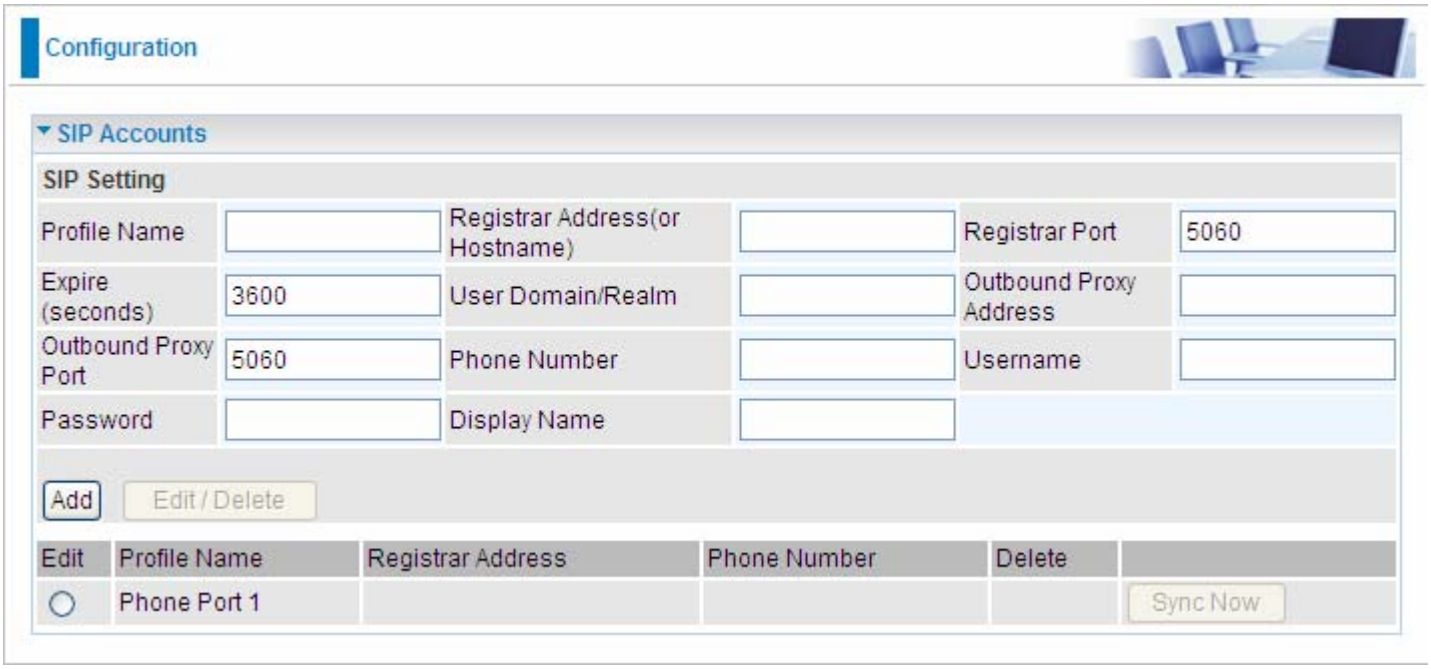
To take your phone OFFHOOK, lift the receiver then press Hook/Flash until you hear your normal PSTN dialtone, not your VoIP dialtone. Wait several seconds and then press Check Level.

You should check the OFFHOOK value for each telephone you have connected to this device. Set the OFFHOOK voltage to the lowest setting registered for all your telephones, e.g. if your telephones return values of 4, 5 and 7 then you should set your OFFHOOK voltage to 4.

Note: The detected values will not automatically be set by the Check Level function; you must enter the lowest level detected after testing all your telephones.

SIP Accounts

This section reflects and contains the basic settings of the VoIP module from the selected provider in the Wizard section. Fail to provide the correct information will stop making calls out to the Internet.



Profile Name: Assign a name for profile identification.

Registrar Address (or Hostname): Indicate the VoIP SIP registrar IP address.

Registrar Port: Specify the port of the VoIP SIP registrar on which it will listen for register requests from VoIP device.

Expire: This is the duration for the registration message being sent.

User Domain/Realm: Set a different domain name for the VoIP SIP proxy server.

Outbound Proxy Address: Indicate the VoIP SIP outbound proxy server IP address. This parameter is very useful when VoIP device is behind a NAT.

Outbound Proxy Port: Specify the port of the VoIP SIP outbound proxy on which it will listen for messages.

Phone Number: This parameter holds the registration ID of the user within the VoIP SIP registrar.

Username: Same as Phone Number.

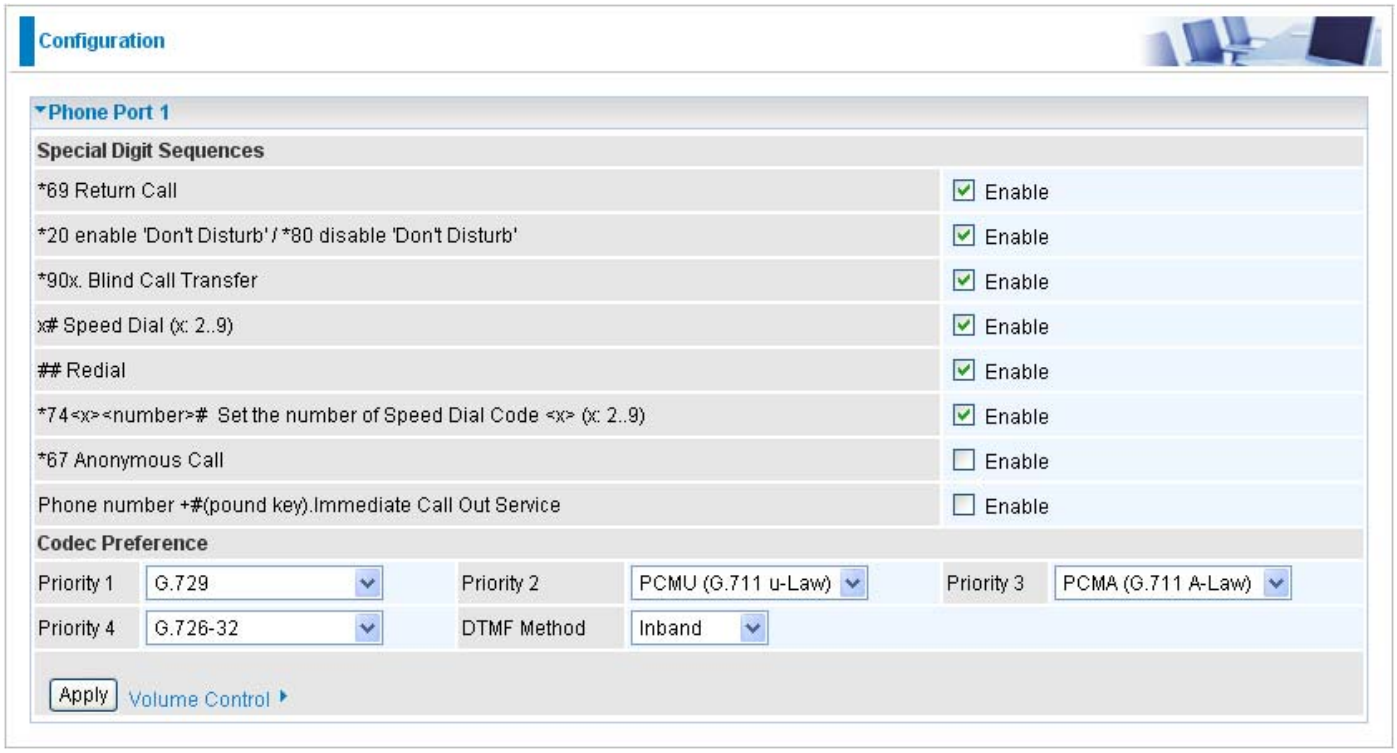
Password: This parameter holds the password used for authentication within the VoIP SIP registrar.

Display Name: This parameter will appear on the Caller ID.

Direct in Dial: Select the ringing port when getting an incoming VoIP call.

Phone Port

This section displays the status and allows for further editing on the account information of the Phones. Click Edit to update your phone information.



Port: It allows you to change the phone port setting for specific FXS port.

***69 (Return Call):** Dial *69 to return the last missed call. It is only available for VoIP call(s).

***20 (Do not Disturb ON):** Dial *20 to enable the No Disturb feature. Your phone will not ring if someone calls.

***90x (Blind Call Transfer):** Dial *90 + phone-number to transfer a call to a third party. This feature is enabled by default.

x# Speed Dial (x:2..9): Refer to the Phone Port section in the Web GUI. Set up your Speed Dial phone book first before accessing the Speed Dial feature. This feature is enabled by default.

Redial: Press ## to redial the latest phone number. This feature is enabled by default.

***74<x><number>#:** Use your phone key pad to insert a phone number to the Speed Dial phone book. Or you can update your Speed Dial phone number manually. Refer to the Phone Port section in the Web GUI for details.

***67 Anonymous Call:** Hide your phone number from being displayed at the remote terminal. It is only applied to the next call when you enter this control character. The detailed operation procedure is “Off Hook -> *67 -> On Hook -> Off Hook -> Dial”. This feature is disabled by default.

Phone Number + #: This is the fast dial which you can dial out a phone number immediately without waiting.

Note: Refer to the Special Dial Code section in this Manual for more details.

Codec Preference

Codec is known as Coder-Decoder, it is used for data signal conversion. Set the priority of voice compression with Priority 1 represents the top priority.

G.729: It is used to encode and decode voice information into a single packet to reduce bandwidth consumption.

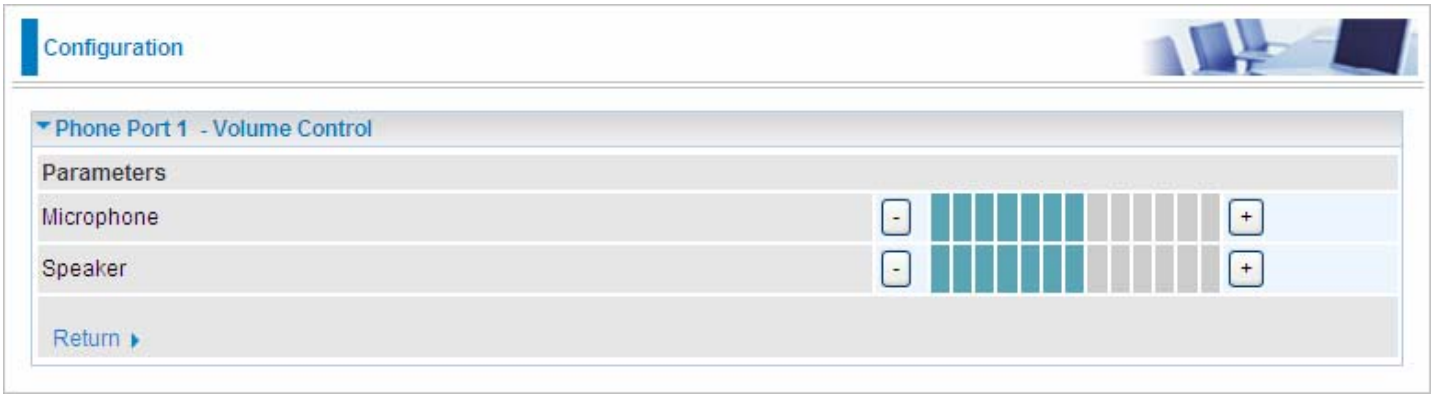
G.711μ-LAW: It is a basic non-compressed encoder and decoder technique. μ-LAW uses pulse code modulation (PCM) encoder and decoder to convert a 14-bit linear sample.

G.711A-LAW: It is a basic non-compressed encoder and decoder technique. A-LAW uses pulse code modulation (PCM) encoder and decoder to convert a 13-bit linear sample.

G.726-32: It is used to encode and decode voice information into a single packet to reduce bandwidth consumption. Currently only support bit rate with 32Kbps.

DTMF Method: The Inband, RFC 2833 and SIP INFO (RFC 2976) are supported.

Volume Control

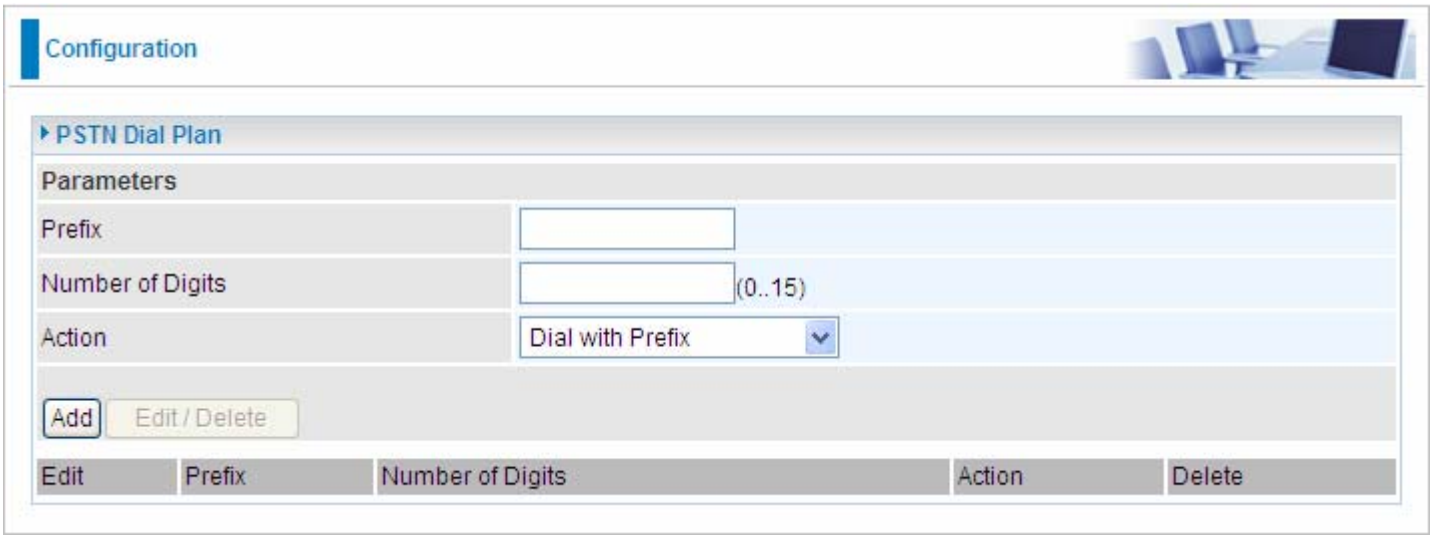


Volume control enables you to adjust the voice quality of telephone to the best & comfortable level. Press “-” the minus sign to reduce either the microphone, speakers level of your telephone or both. Press “+”, the plus sign to increase either the microphone, speakers level of your telephone or both.

PSTN Dial Plan (Router with LINE port only)

This section enables you to configure the “VoIP with PSTN switching” on your system. You can define a range of dial plans that will make regular call to switch from VoIP to PSTN line. Prefix number is an essential key to make a difference between VoIP and Regular phone call. If the actual numbers dialed match with the prefix number defined in this dial plan, the dialed number will be rerouted to the PSTN to make a regular call. Otherwise, the number will be rerouted to the VoIP networks.

Note: In order to utilize this feature, you must have registered and connected to your SIP Server first.



Prefix: Specify the number(s) that will be used to switch from VoIP to PSTN when making a call.

Number of Digits: Specify the total number of digits you wish to dial out. The maximum number of digit is 15.

Action: Specify a dialing method that you wish to use when making PSTN call(s).

Dial with Prefix: With this selected, the prefix which is dialed together with the phone number will be dialed out as well via FXO when making a regular call.

Note: The prefix number dialed has to match the number of digit specified.

Dial without Prefix: With this selected, the prefix which is dialed together with the phone number will not be dialed out with the phone number via FXO when making a regular call.

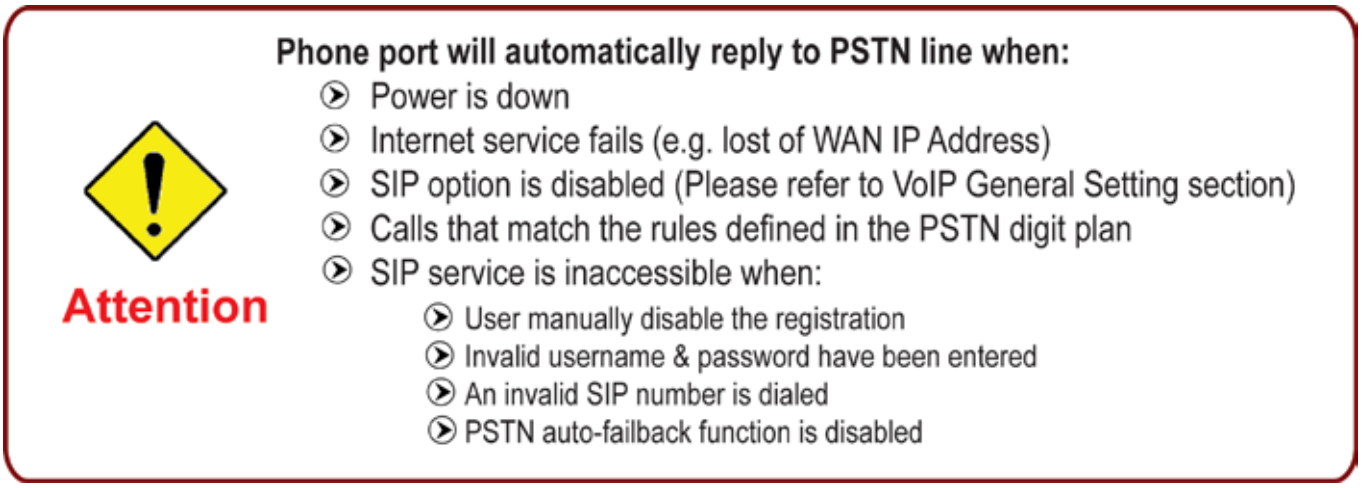
Note: The length of the number of digit dialed should match the number of digit specified.

Dial at Timeout: The number & the prefix entered will be dialed out via the FXO port after a defined timeout interval although the number of digits of the phone number entered does not match the number of digits specified.

Note: The length of the number of digit dialed must not exceed the number of digit defined otherwise dialing will be invalid.

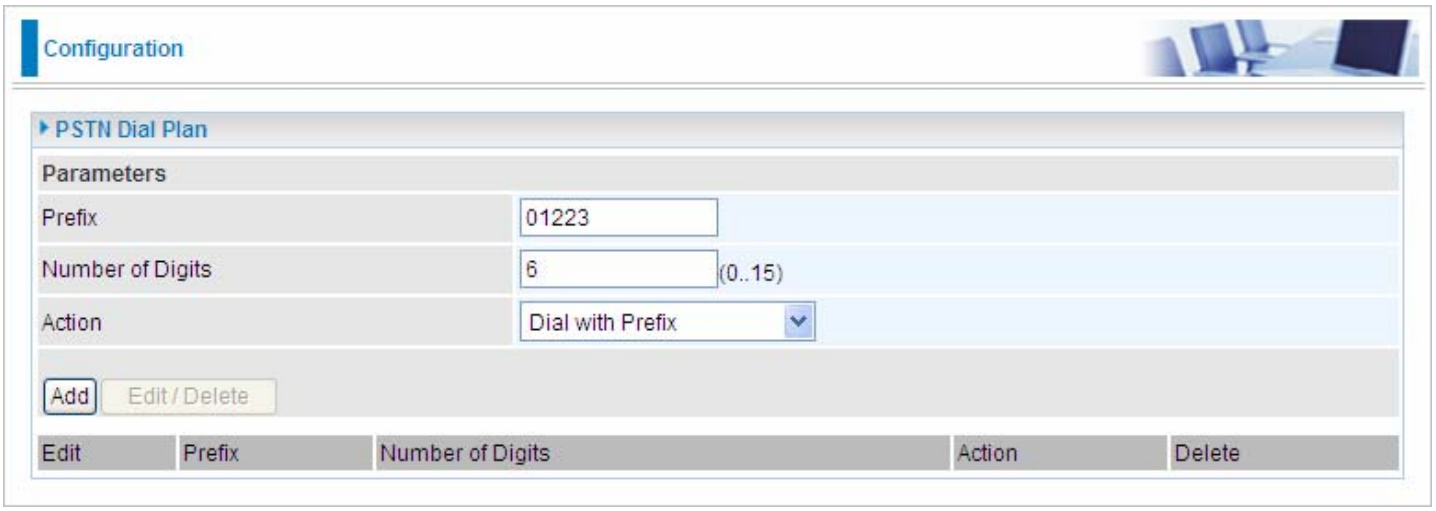
Dial at Timeout no Prefix: The phone number & the prefix entered will be dialed out via the FXO port excluding the prefix after a defined timeout interval although the number of digit of the phone number entered does not match the number of digit specified.

Note: The length of the number of digit dialed must not exceed the number of digit defined otherwise dialing will be invalid.


Attention
Phone port will automatically reply to PSTN line when:
Power is down
Internet service fails (e.g. lost of WAN IP Address)
SIP option is disabled (Please refer to VoIP General Setting section)
Calls that match the rules defined in the PSTN digit plan
SIP service is inaccessible when:
User manually disable the registration
Invalid username & password have been entered
An invalid SIP number is dialed
PSTN auto-failback function is disabled

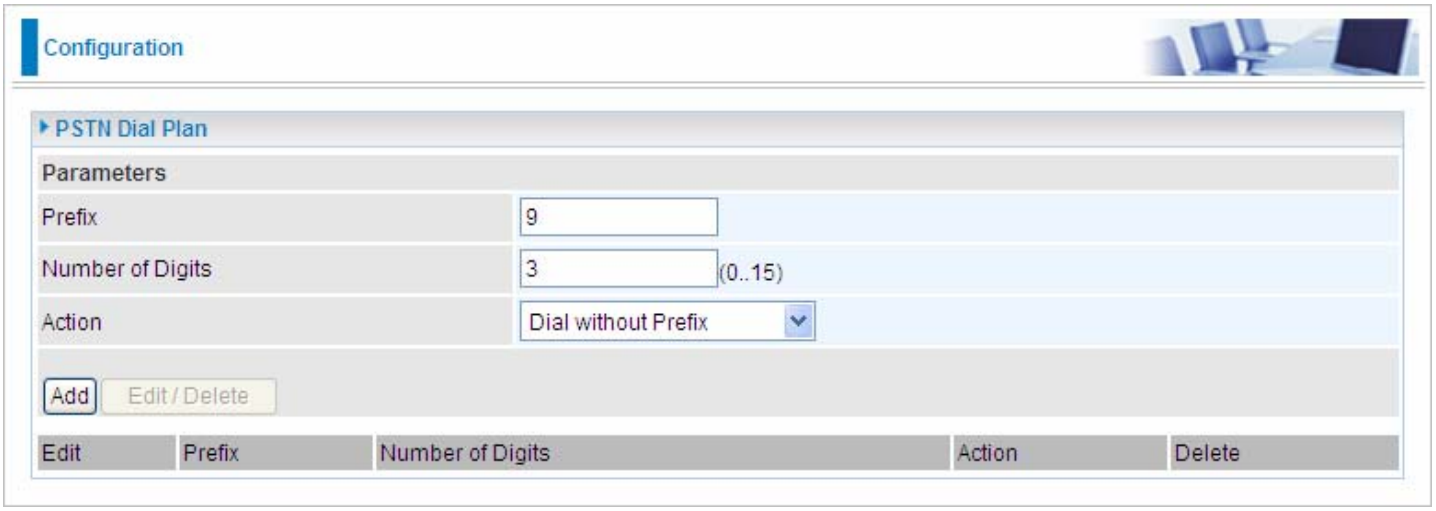
PSTN Dial Plan Examples:

1. Dial with Prefix



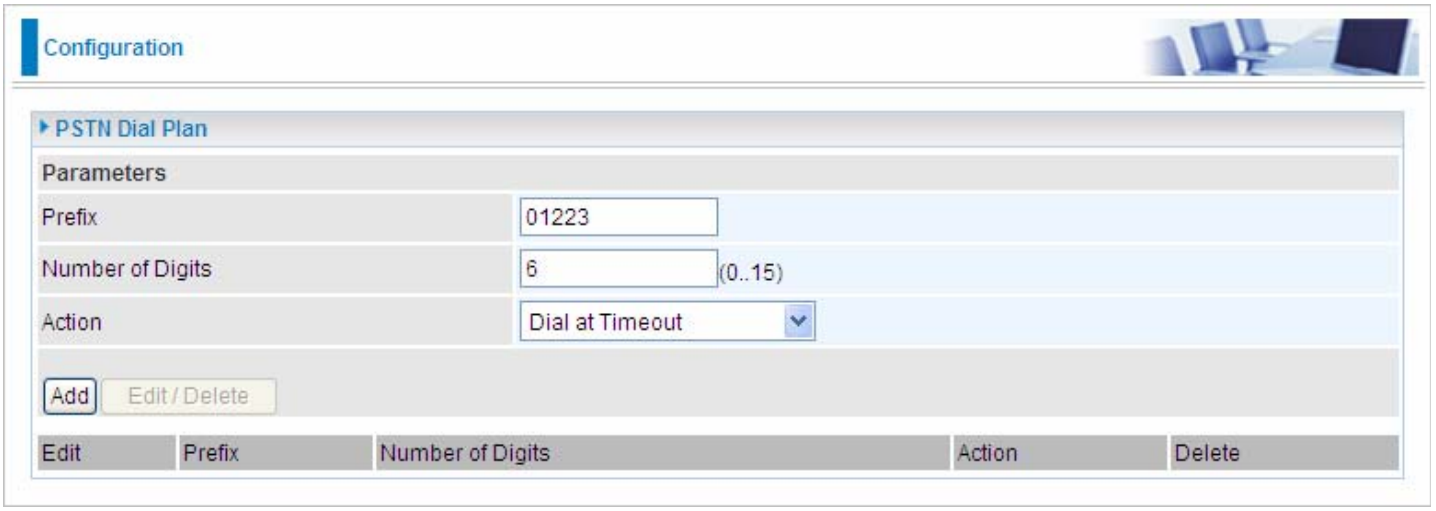
If you dial 01223 707070, the number 01223707070 will be dialed out via FXO for making a regular phone call.

2. Dial without Prefix



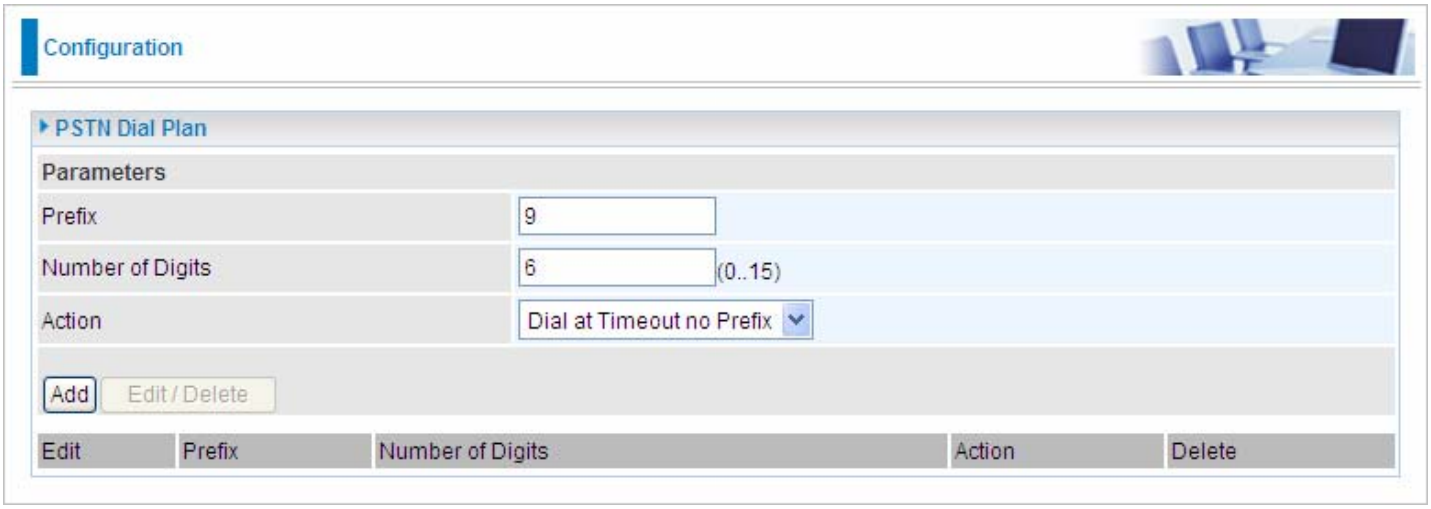
If you dial 9102, only 102 will be dialed out via FXO port for making a regular phone call.

3. Dial at Timeout



If you only dial 01223 7070, the number 012237070 will be dialed to make a regular call via FXO port after a defined timeout interval even though the number of digit entered does not match the number of digit defined. Number 7070 will still be a valid number for the device to complete the dialing because it does not exceed the number of digit defined.

4. Dial at Timeout no Prefix



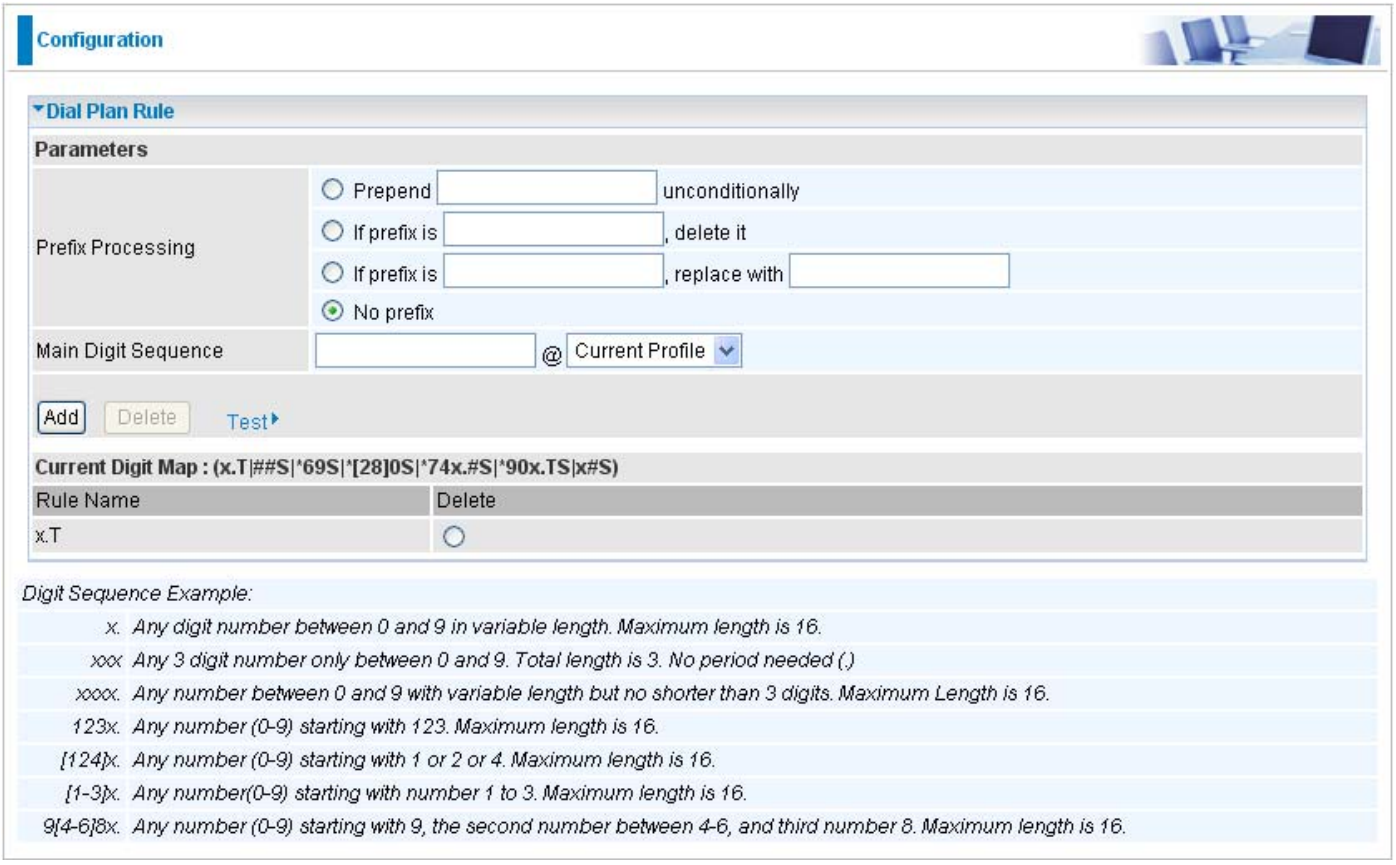
If you only dial 97070, the number that is dialed out via FXO port for making a regular call will not have its prefix. Even though 7070 (only 4 digits) does not match the number of digit defined in the field, 7070 is still a valid phone number since it has not exceeded the number of digit defined.

VoIP Dial Plan

This feature makes dialing phone number a lot more convenient and easy. Instead of having to memorize long digits of every single contact, VoIP Dial Plan provides you the ease to create dial plans that will enable you to make your phone calls without the need to memorize the phone number. To access this feature, go to Configuration > VoIP > VoIP Dial Plan.

Dial Plan Rules

Click the Add button to create and define a VoIP dial plan rule.


Configuration
Dial Plan Rule
Parameters
Prefix Processing
Prepend
unconditionally
If prefix is
, delete it
If prefix is
, replace with
No prefix
Main Digit Sequence
@
Current Profile
Add
Delete
Test
Current Digit Map : (x.T|##S|*69S|*[28]0S|*74x.#S|*90x.TS|x#S)
Rule Name
Delete
x.T
Digit Sequence Example:
x. Any digit number between 0 and 9 in variable length. Maximum length is 16.
xxx Any 3 digit number only between 0 and 9. Total length is 3. No period needed (.)
xxxx. Any number between 0 and 9 with variable length but no shorter than 3 digits. Maximum Length is 16.
123x. Any number (0-9) starting with 123. Maximum length is 16.
[124]x. Any number (0-9) starting with 1 or 2 or 4. Maximum length is 16.
[1-3]x. Any number(0-9) starting with number 1 to 3. Maximum length is 16.
9[4-6]8x. Any number (0-9) starting with 9, the second number between 4-6, and third number 8. Maximum length is 16.

Prefix Processing:

Prepend xxx unconditionally: xxx number is appended unconditionally to the front of the dialing number when making a call. Prefix can also be included with any number and/or character such as +, *, #.

Note: For special service with +, *, #, you may need to check with your VoIP or Local Telephone Service Provider for information.

If Prefix is xxx, delete it: Prefix xxx is removed from the dialing numbers before making a call.

If Prefix is xxx, replace with: Prefix xxx is appended to the front of the dialing numbers when making a call.

No prefix: No prefix is appended to the front of the numbers dialed. This is the default setting for Prefix Processing section.

Main Digit Sequence: The call(s) can be called out via SIP, PSTN or ENUM. x: Any numeric number between 0 and 9.
. (period): Repeat numeric number(s) between 0 and 9.

*** (asterisk sign):** It is a normal character '*' on the phone key pad. Please check if any special service is provided by your VoIP Service Provider or your Local Telephone Service Provider.

 # (pound sign): It is a normal character '#' on the phone key pad. Please check if any special service is provided by your VoIP Service Provider or the Local Telephone Service Provider.

<@ Current Profile>: Refer to the VoIP account registered on the *VoIP Wizard* for Port 1.

<@ PSTN>: Making a telephone call via the PSTN line.

<@ENUM>: Making a VoIP SIP direct call via an Electronic number (ENUM) 164 to an ENUM callee.
Electronic Number (ENUM) uses DNS (Domain Network System) based technology to map between a traditional phone number (PSTN) to an Internet addresses/ SIP URL. The ENUM number must be registered via a public ENUM site or your VoIP Service Provider.

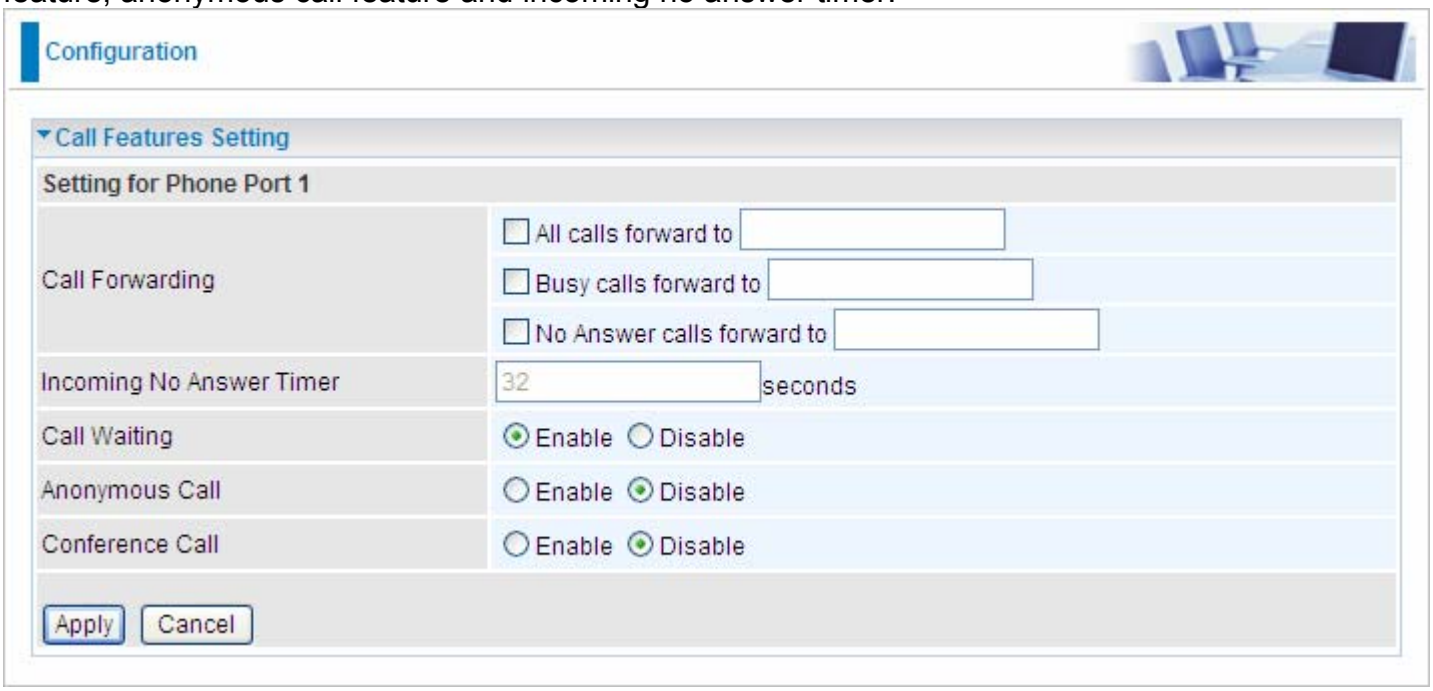
<@ SIPgateway>: It is used for the Intelligent Call Routing feature where you need to set up your SIP account on the VoIP User defined Profiles link on the VoIP Wizard page. Go to the VoIP Wizard in this manual for more information.

Dial-Plan Examples:	**Description**
x	Any digit number between 0 and 9 in variable length. Maximum length is 16.
xxx	Any 3 digit number only between 0 and 9. Total length is 3. ***Note: No period is needed (.)***
xxxx	Any number between 0 and 9 with variable length but no shorter than 3 digits. Maximum length is 16.
123x	Any number (0-9) starting with 123. Maximum length is 16.
[x…x]x. For example: [124]x.	Any number (0-9) starting with 1 or 2 or 4. Maximum length is16.
[x-x]x. For example: [1-3]x.	Any number (0-9) starting with number 1 to 3. Maximum length is 16.
x[x-x]x. For example: 9[4-6]8x.	Any number (0-9) starting with 9, the second number between 4-6, and third number 8. Maximum length is 16.
Special Dial Plan Examples:	**Description**
*xx*x	Starting with '* sign' + any two digit numbers + any number (0-9) in variable length. Maximum length is 16.
*xx	Starting with '* sign' + any 2 digit numbers between 0 and 9. Total length including the * is 3. ***Note: No period is needed (.)***

**xx*x.	Starting with '** sign' + any two digit numbers between 0 + any number (0-9) in variable length. Maximum length is 16.
#xx.	Starting with '# sign' + any digit number (0-9) in variable length but no shorter than 1 digits. Maximum length is 16.
##xx*x.	Starting with '## sign' + any two digit numbers + '* sign' + any number (0-9) in variable length. Maximum length is 16.

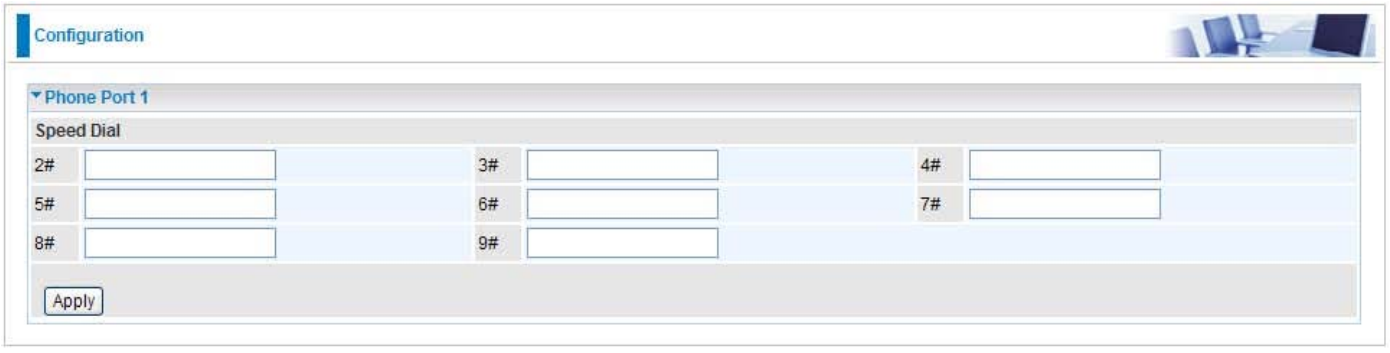
Call Feature

VoIP has all the basic features of a traditional phone. Besides the provided basic features, VoIP also comes with several enhanced features that allows you to further customize their settings to suit your personal needs such as call forwarding setting, call waiting time length, conference call feature, anonymous call feature and incoming no answer timer.



Speed Dial

Speed Dial comes in handy to store frequently used telephone numbers which you can press number from 0 to 9 and the pound sign (#) on the phone keypad to activate the function. For example, speed dial to phone number lists on 9, just press keypad 9 then #. Your router will automatically call out to number listed on entry 9.



Ring & Tone

This section allows advanced user to change the existing or newly defined parameters for various ring tones (dial tone, busy tone, answer tone and etc.)

Configuration

Ring & Tone Configuration

Country Specific Ring & Tone											
Region	USA										
Ring Parameters											
	On 1	Off 1	On 2	Off 2	On 3	Off 3					
Ring Cadence (in ms)	2000	4000	0	0	0	0					
Tone Parameters											
	Harmonica		Harmonica		Cadence						
	Freq. 1	Power 1	Freq. 2	Power 2	On 1	Off 1	Repeat 1	On 2	Off 2	Repeat 2	
Dial Tone	350	-13	440	-13	1000	0	-1	0	0	0	
Ringback Tone	440	-19	480	-19	2000	4000	-1	0	0	0	
Busy Tone	480	-24	620	-24	500	500	-1	0	0	0	
Alerting Tone	440	-13	0	0	2000	10000	1	500	10000	1	
Answer Tone	440	-13	0	0	1000	0	1	0	0	0	
Calling Card "Bong" Tone	941	-20	1477	-20	30	0	1	30	0	1	
Call Waiting Tone	440	-30	0	0	400	0	1	0	0	0	
Confirm Tone	350	-13	440	-13	100	100	3	0	0	0	
Error Tone	985	-20	1370	-20	380	1	1	274	1	1	
Intercept Tone	440	-24	620	-24	250	0	1	0	0	0	
Message Waiting Tone	350	-13	440	-13	100	100	15	1000	0	-1	
Network Busy Tone	480	-24	620	-24	250	250	-1	0	0	0	
Network Congestion Tone	480	-24	620	-24	250	250	-1	0	0	0	
Off Hook Warning Tone	1400	-4	2060	-4	100	100	-1	0	0	0	
Preemption Tone	440	-13	0	0	1000	0	1	0	0	0	
Prompt Tone	941	-20	1477	-20	30	0	1	30	0	1	
Reorder Tone	480	-24	620	-24	250	250	-1	0	0	0	
Reorder Warning Tone	1400	-20	0	0	500	15000	-1	0	0	0	
Ringback on Connection Tone	440	-19	480	-19	2000	3000	1	2000	3000	1	
Silence Tone	0	0	0	0	0	0	0	0	0	0	
Stutter Dial Tone	350	-13	440	-13	100	100	3	100	100	-1	

Apply Cancel

Country Specific Ring & Tone

Region: Select a country ring tone from the drop-down list that pertains to your residence. This VoIP router will display the default parameters of each ring tone according to the country selected. If your country is not found in the list, you may manually enter the parameters of the ring tone that pertains to the country.

Ring Parameters

Ring Cadence (in ms): Ring cadence is defined by three fields, Frequency: On Time1, Off Time1, On Time2, Off Time2 and On Time3, Off Time3. Frequency is specified in Hertz. Time is given in milliseconds.

Tone Parameters

You may need to check with your local telephone service provider for such information. Also, it is recommended that this option be configured by an advanced user unless you are instructed to do so.

Click **Apply** to apply the settings.

QoS - Quality of Service

QoS function helps you to control the network traffic of each application from LAN (Ethernet and/ or Wireless) to WAN (Internet). It facilitates you the features to control the quality and speed of throughput for each application when the system is running with full upstream load.

These are the items within the QoS section: **Prioritization, Outbound IP Throttling & Inbound IP Throttling (bandwidth management).**

Prioritization

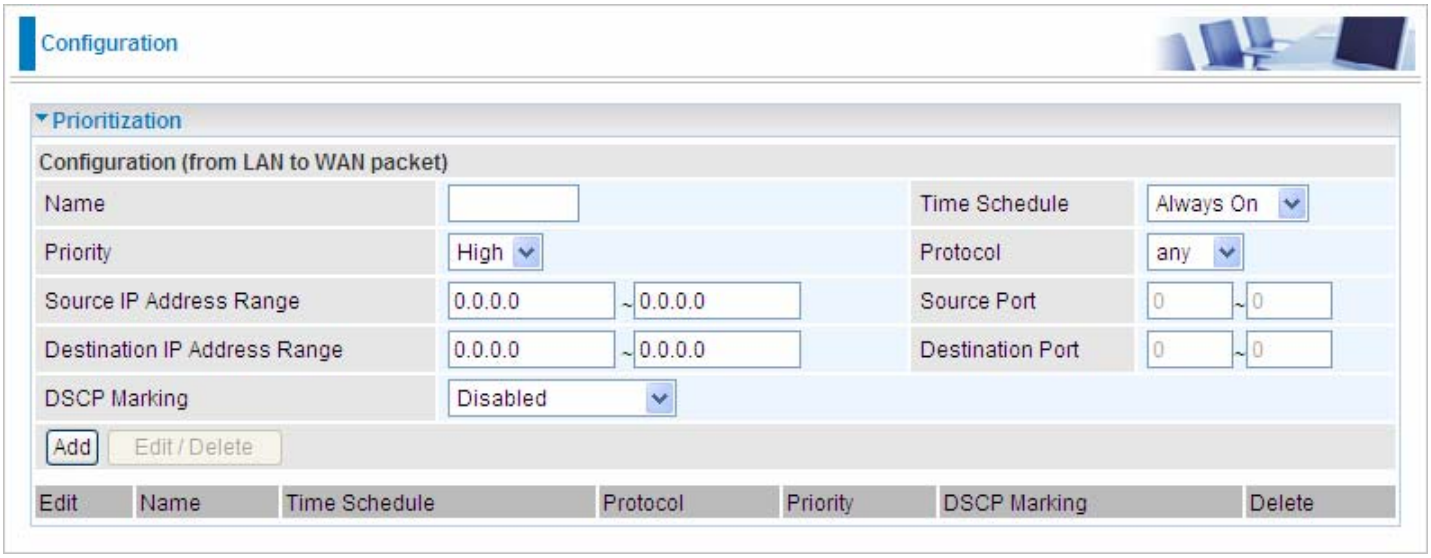
There are three priority settings to be provided in the Router:

High

Normal (The default is normal priority for all of traffic without setting)

Low

The utilization percentage of each priority settings are High (60%), Normal (30%) and Low (10%). To delete an application, you can click on the Delete radio button of the application and then click the Edit/Delete button.



Name: User defined description to identify the new policy/application created.

Time Schedule: Schedule your prioritization policy.

Priority: The priority given to each policy/application. Its default setting is set to High. You may adjust this setting to fit your policy / application.

Protocol: The name of the supported protocol.

Source IP Address Range: The source IP address or the range of the packets to be monitored.

Source Port: The source port of the packets to be monitored.

Destination IP address Range: The destination IP address or range of packets to be monitored.

Destination Port: The destination port of the packets to be monitored.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value. See Table 4 for **DSCP Mapping Table**.

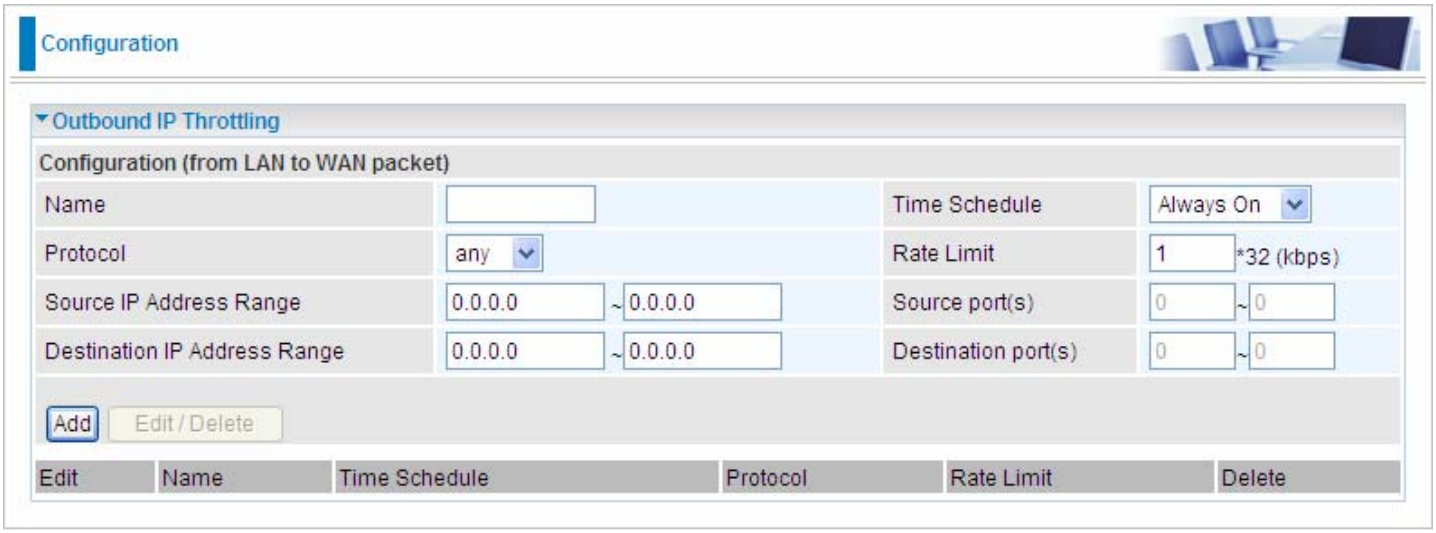
Note: Make sure that the router(s) in the network backbone are capable to execute and check the DSCP throughout the QoS network.

Table 4: DSCP Mapping Table

DSCP Mapping Table	
(Wireless) ADSL Router	**Standard DSCP**
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

Outbound IP Throttling (LAN to WAN)

IP Throttling allows you to limit the speed of the IP traffic. The value entered in the Rate Limit blank will set the speed limitation of the application.



Name: User defined description to identify the new policy/name created.

Time Schedule: Schedule your prioritization policy. Refer to **Time Schedule** for more information.

Protocol: The name of the supported protocol.

Rate Limit: To limit the speed of the outbound traffic.

Source IP Address Range: The source IP address or the range of packets to be monitored.

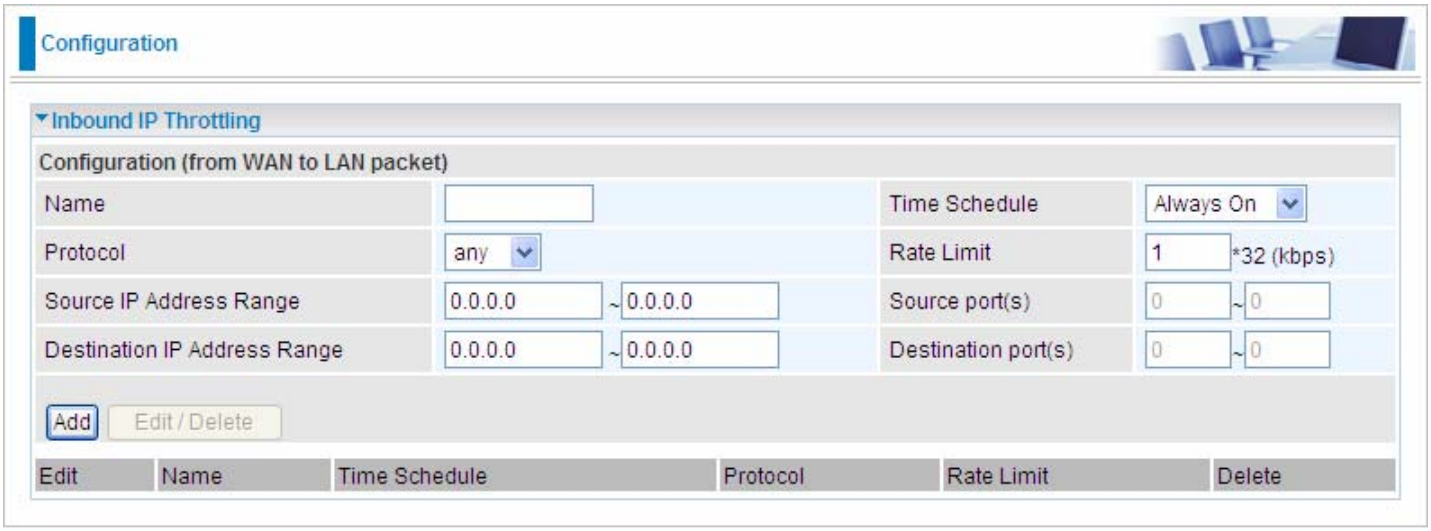
Source Port(s): The source port of the packets to be monitored.

Destination IP Address Range: The destination IP address or the range of packets to be monitored.

Destination Port(s): The destination port of the packets to be monitored.

Inbound IP Throttling (WAN to LAN)

IP Throttling allows you to limit the speed of the IP traffic. The value entered in the Rate Limit blank will set the speed limitation of the application.



Name: User defined description to identify the new policy/application created.

Time Schedule: Schedule your prioritization policy. Refer to **Time Schedule** for more information.

Protocol: The name of the supported protocol.

Rate Limit: To limit the speed of the inbound traffic.

Source IP Address Range: The source IP address or the range of the packets to be monitored.

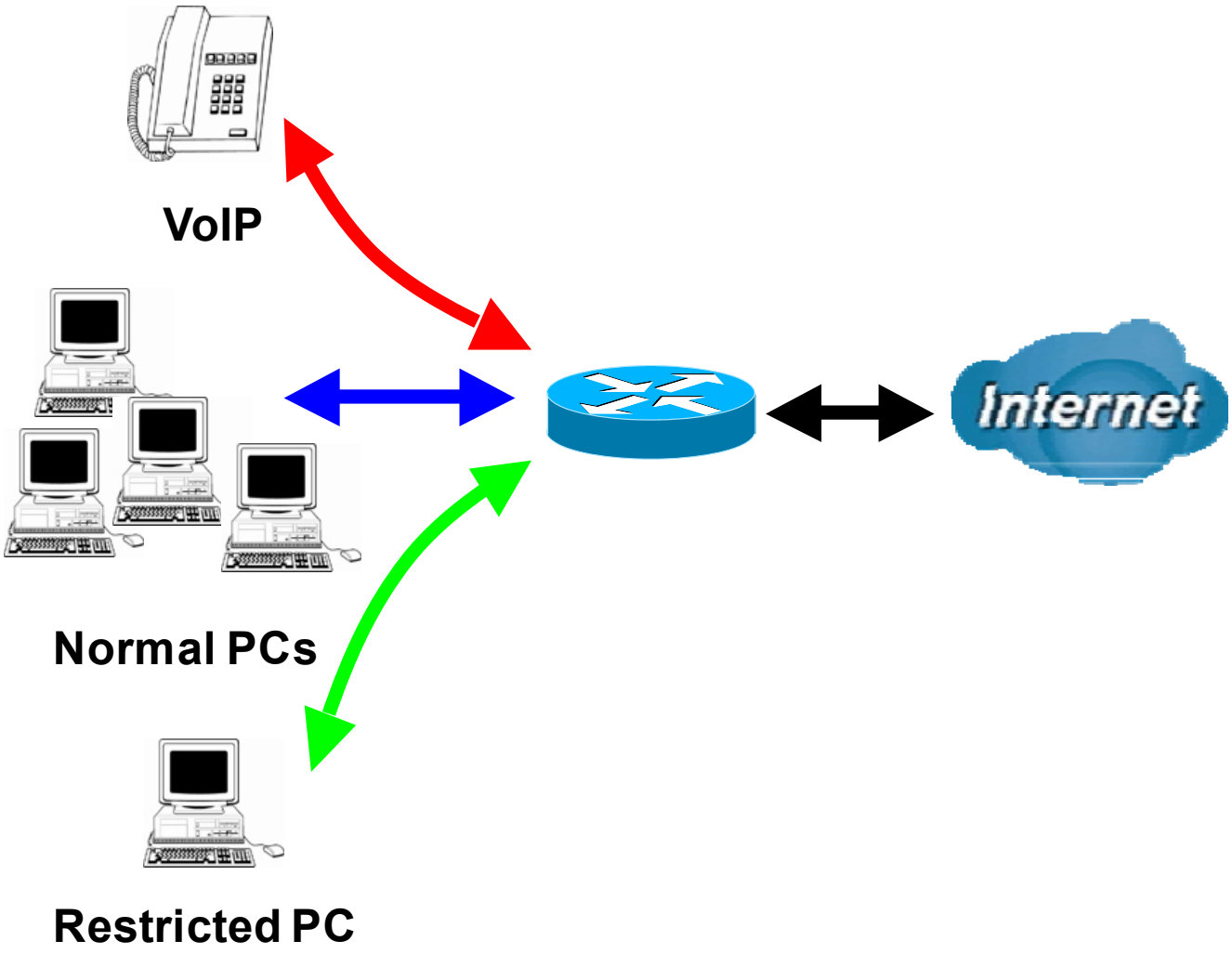
Source Port(s): The source port of the packets to be monitored.

Destination IP Address Range: The destination IP address or the range of the packets to be monitored.

Destination Port(s): The destination port of the packets to be monitored.

Example: QoS for your Network

Connection Diagram



Information and Settings

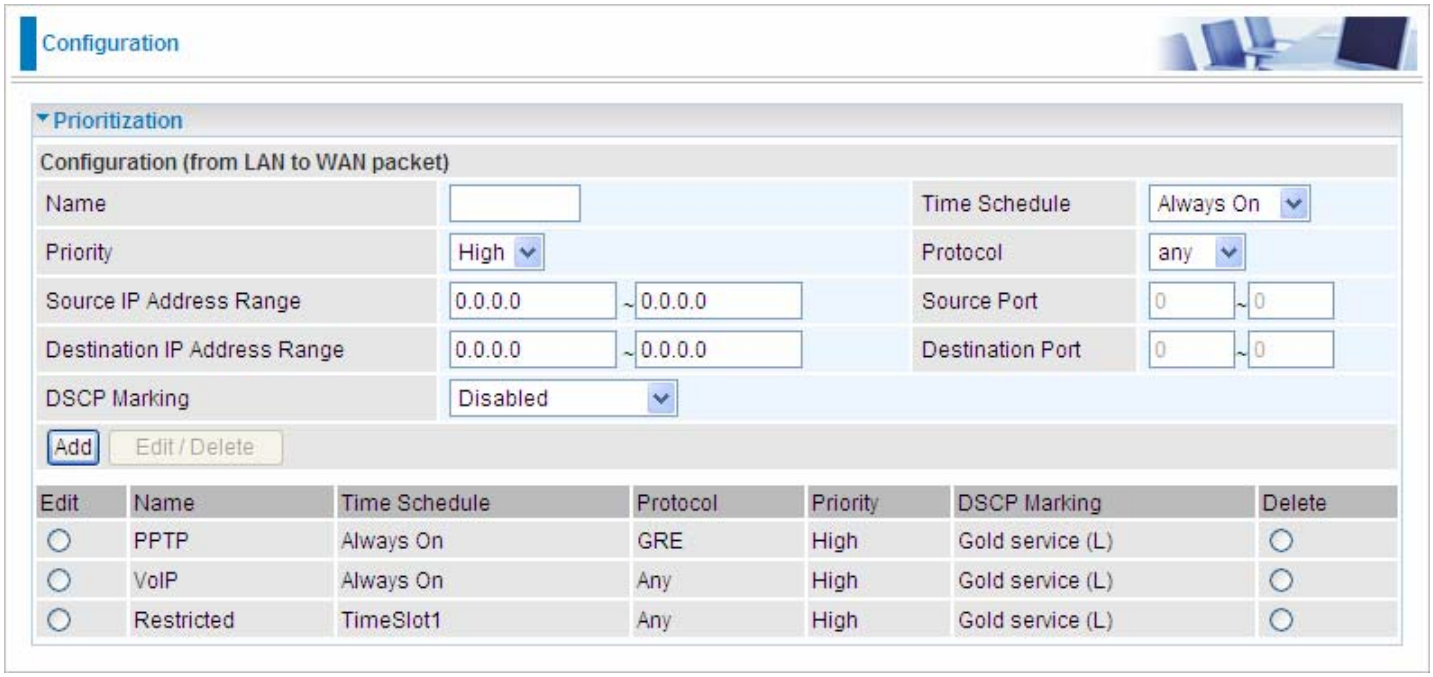
Upstream: 928 kbps

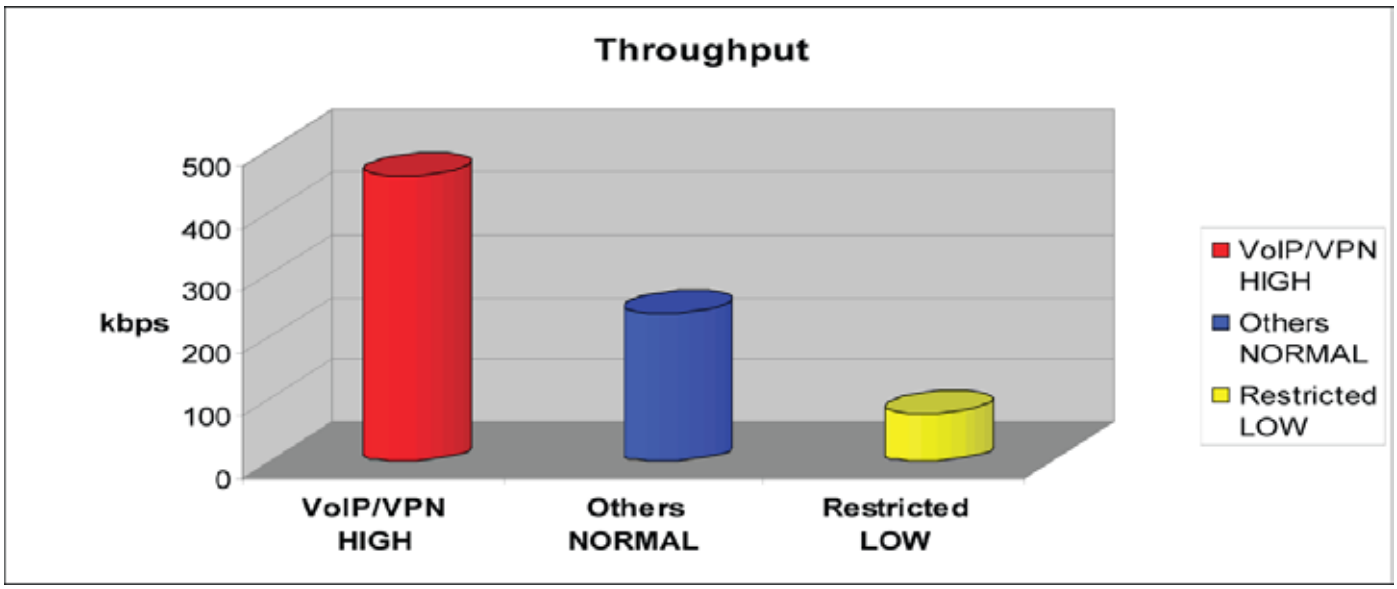
Downstream: 8 Mbps

VoIP User : 192.168.1.1

Normal Users : 192.168.1.2~192.168.1.5

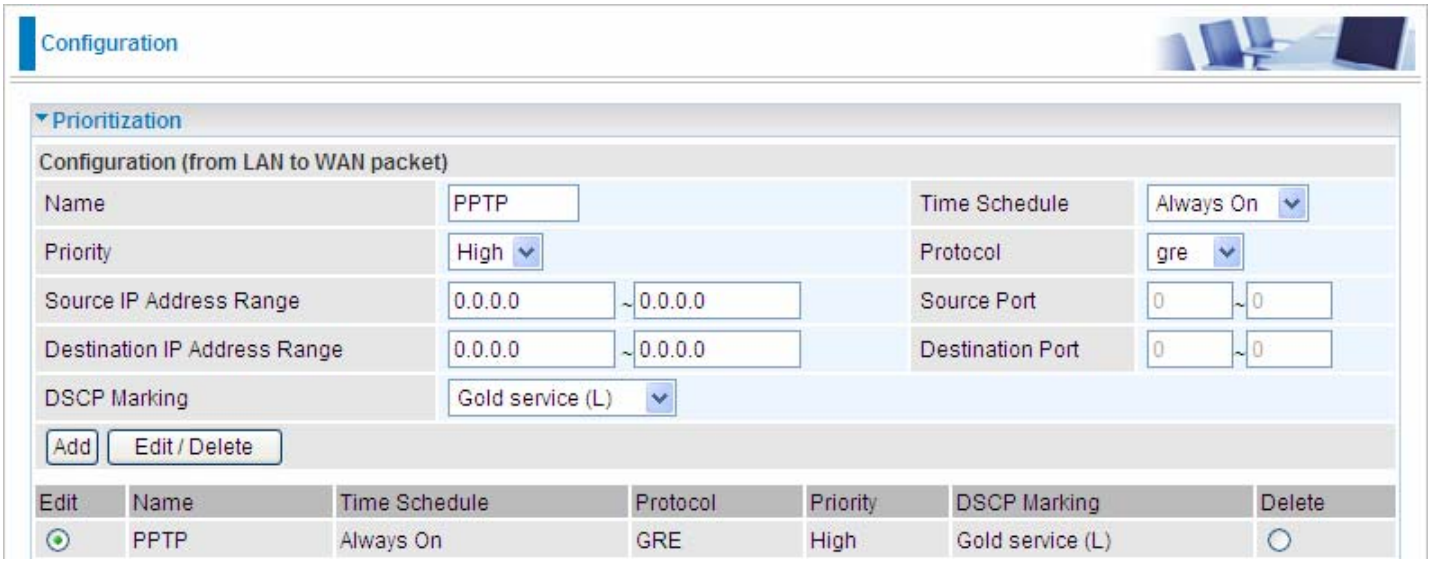
Restricted User: 192.168.1.100





Mission-critical application

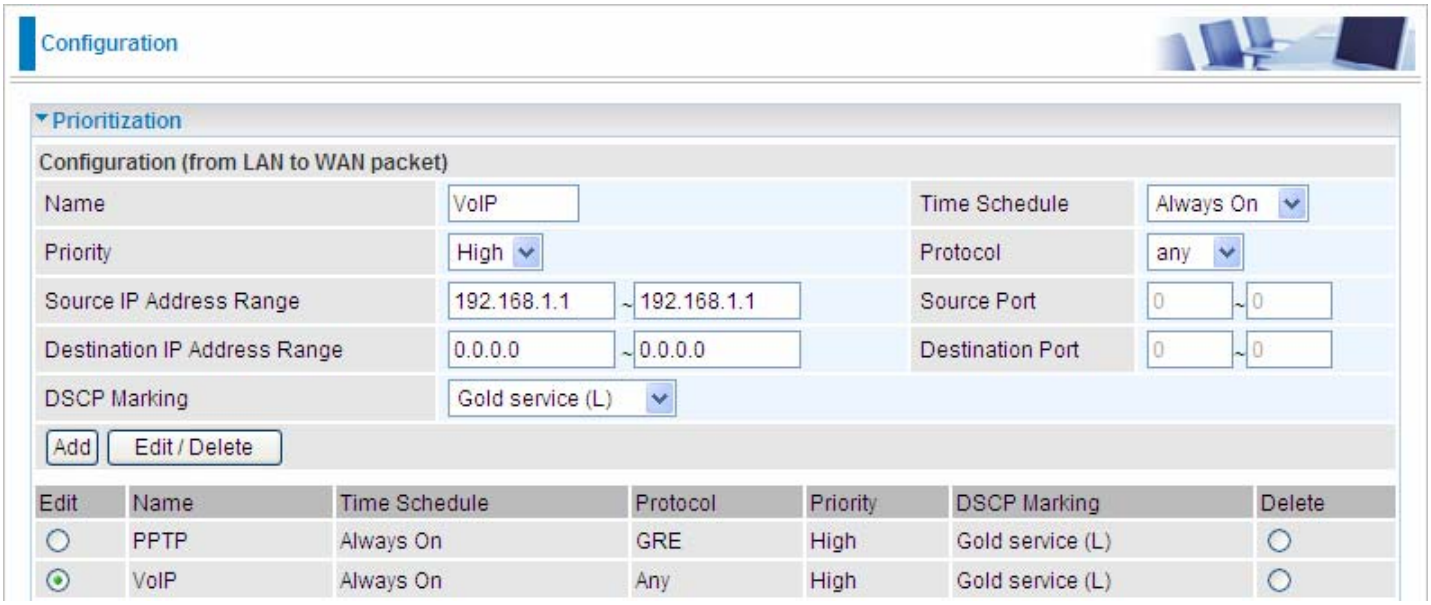
Mostly the VPN connection is mission-critical application for doing data exchange between head and branch office.



The mission-critical application must be sent out smoothly without any drop out. Set the level of priority as high to prevent other applications from saturating the bandwidth.

Voice application

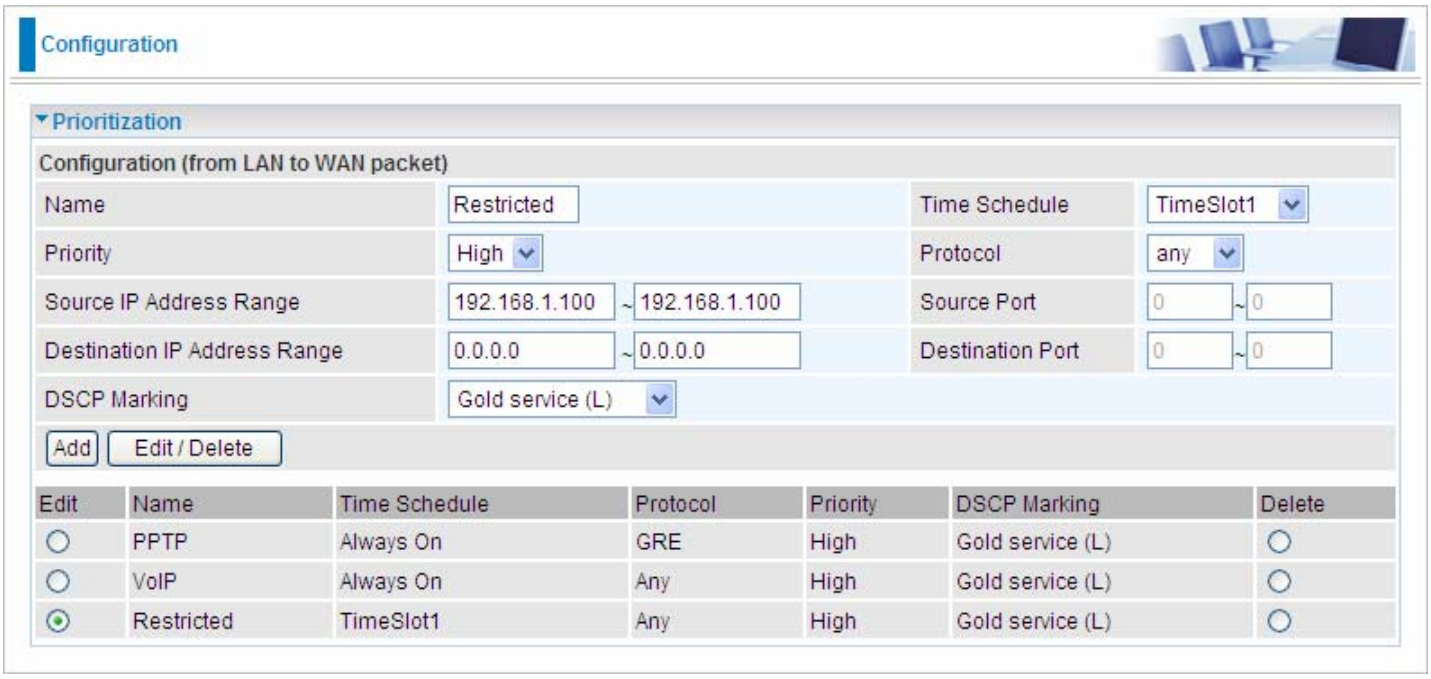
Voice is latency-sensitive application. Most VoIP devices are use SIP protocol and the port number will be assigned by SIP module automatically. Better to use fixed IP address for catching VoIP packets as high priority.



The setting above will help to improve the quality of your VoIP service when the traffic is fully loaded.

Restricted Application

Some companies will setup their FTP servers for data download while others may use FTP for file sharing.



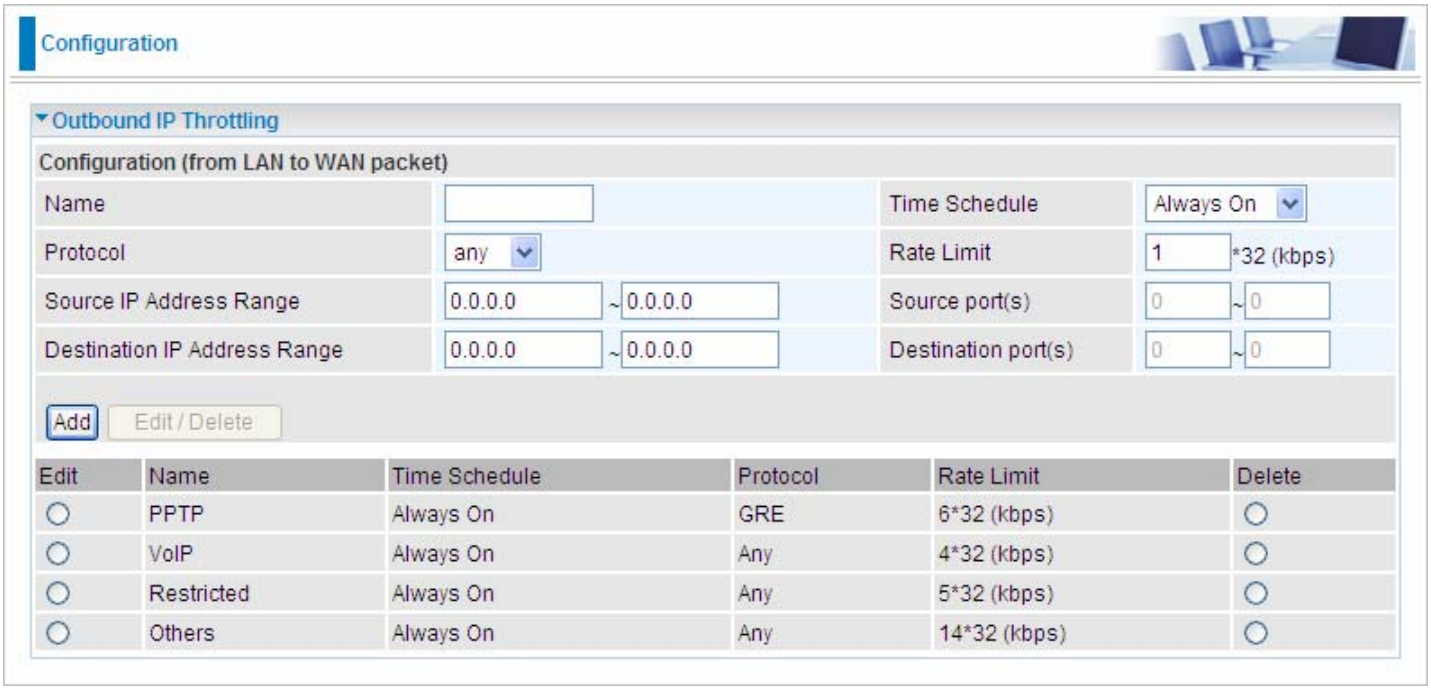
The setting above helps to limit the utilization of the FTP upstream rate. Time schedule also helps to limit its utilization only during daytime.

Advanced setting by using IP throttling

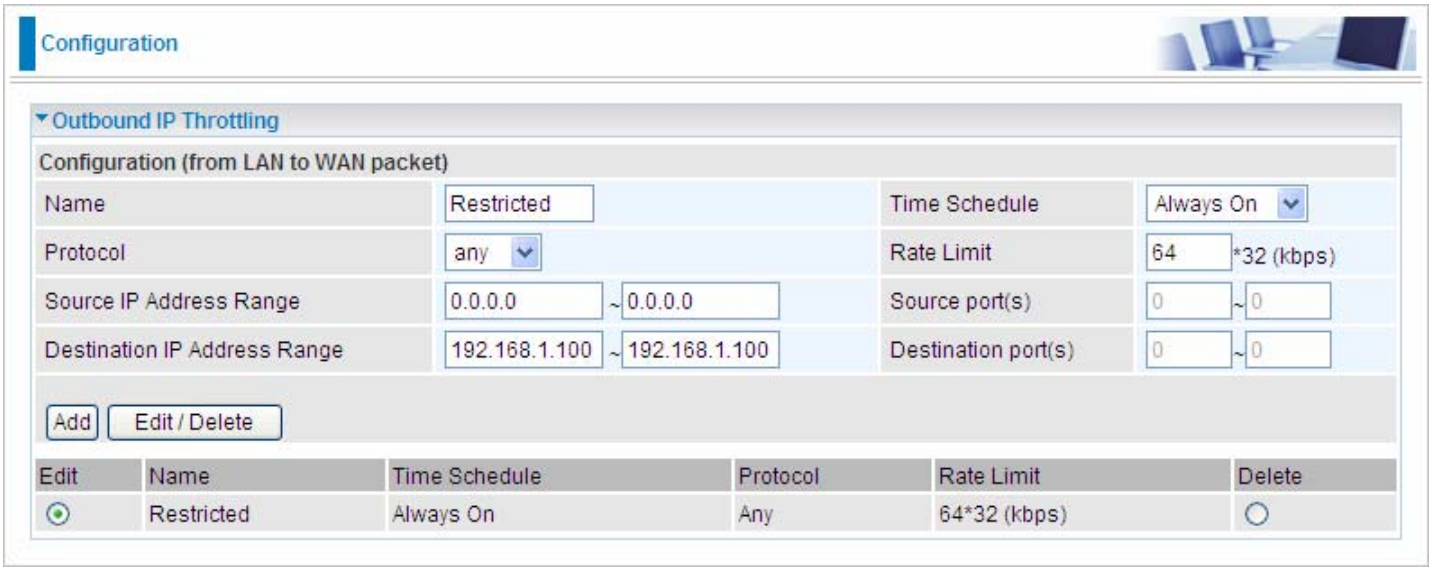
IP throttling enables you to set parameters for bandwidth allocation, although the applications maybe located on the same level.

Upstream: 928kbps (29*32kbps)

Mission-critical Application: 192kbps (6*32kbps)
Voice Application: 128kbps (4*32kbps)
Restricted Application: 160kbps (5*32kbps)
Other Applications: 448kbps (14*32kbps)
6+4+14+5=29, 29*32kbps=928kbps



Sometime your customers or friends may upload their files to your FTP server and that will saturate your downstream bandwidth. The settings below help you to limit bandwidth for the restricted application.



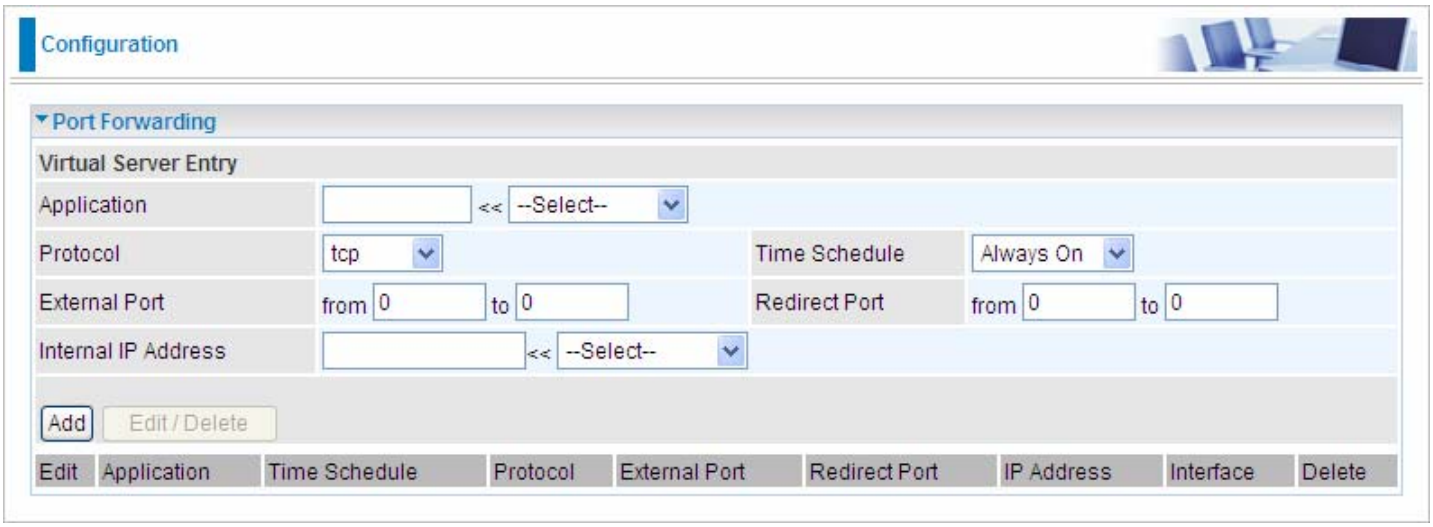
Virtual Server (known as Port Forwarding)

In TCP/IP and UDP networks, a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the WAN configuration section of this manual for more information on NAT.

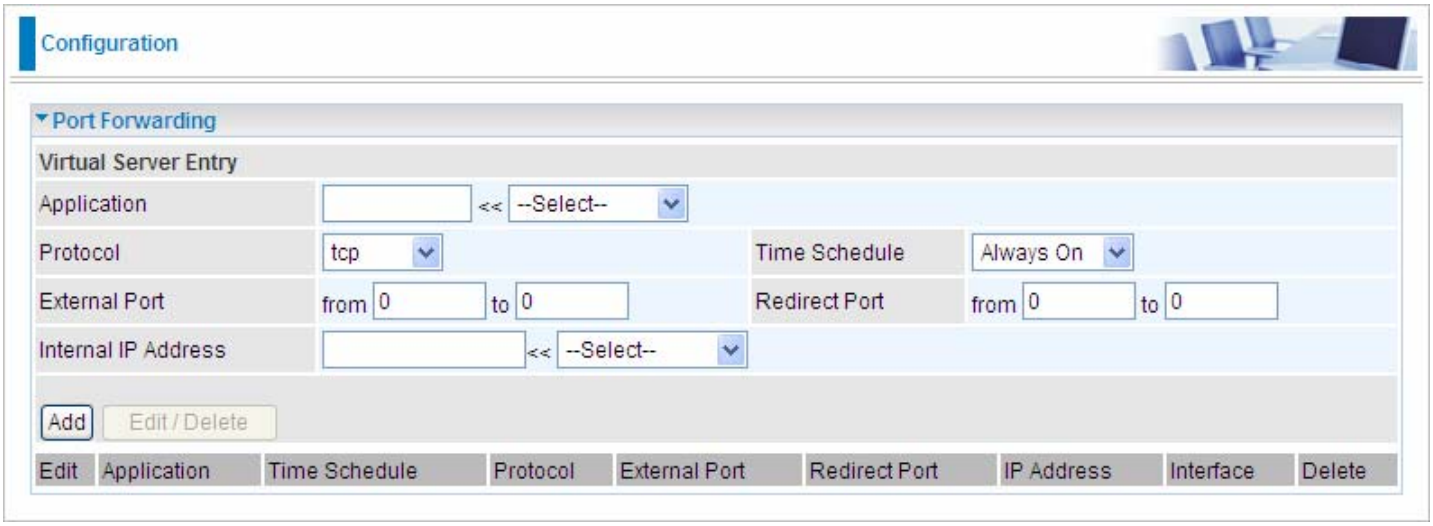
The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.



Add Virtual Server

Because NAT can act as a “natural” Internet firewall, your router protects your network from being accessed by outside users when using NAT, as all incoming connection attempts will point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network.

When your router needs to allow an outside user to access the internal server, e.g. a web server, FTP server, Email server or game server, the router can act as a virtual server. You can set up a local server with a specific port number for this service, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request to the router for a specified port is received, it will be forwarded to the corresponding internal server.



Application: User defined description to identify this entry or click the Application drop-down menu to select an existing predefined rules.

--Select-- : 20 predefined rules are available. Application, Protocol and External/Redirect Ports will be filled after the selection.

Protocol: It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by a particular application. Most applications will use TCP or UDP.

Time Schedule: User defined time period to enable your virtual server. You may specify a time schedule or select “Always on” for this Virtual Server Entry. For setup and detail, refer to **Time Schedule** section.

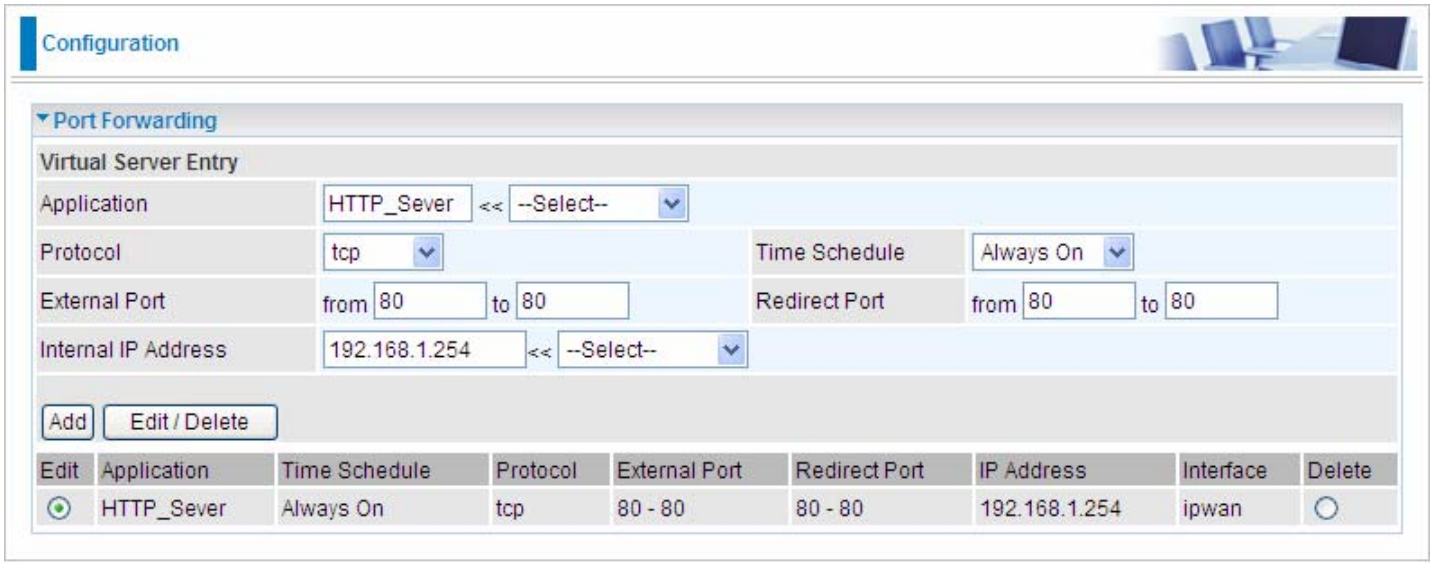
External Port: The Port number on the Remote/WAN side used when accessing the virtual server.

Redirect Port: The Port number used by the Local server in the LAN network.

Internal IP Address: The private IP in the LAN network, which will be providing the virtual server application. --Select-- List all existing PCs connecting to the network. You may assign a PC with IP address and MAC from this list.

Example:
If you like to remotely access your Router through the Web/HTTP all the time, you will need to enable port number 80 (Web/HTTP) and map to the Router's IP Address. Then all incoming HTTP requests from you (Remote side) will be forwarded to the Router with an IP address of 192.168.1.254. Since port number 80 has already been predefined, next to the Application click Helper. A window with a list of predefined rules will pop, you can then select HTTP_Sever.

Application: *HTTP_Sever* Time Schedule: *Always On* Protocol: *tcp*
External Port: *80-80*
Redirect Port: *80-80*
IP Address: *192.168.1.254*



Add: Click it to apply your settings.

Edit/Delete: Click it to edit or delete this virtual server application.

NOTE:

Using Port Forwarding does have implications, as outside users will be able to connect to the PCs on your network. For this reason, you are adviced to use specific Virtual Server entries just for the port your application requires instead of using DMZ. Doing so will result in all connections from WAN to attempt to access the public IP your DMZ specifies.

Attention

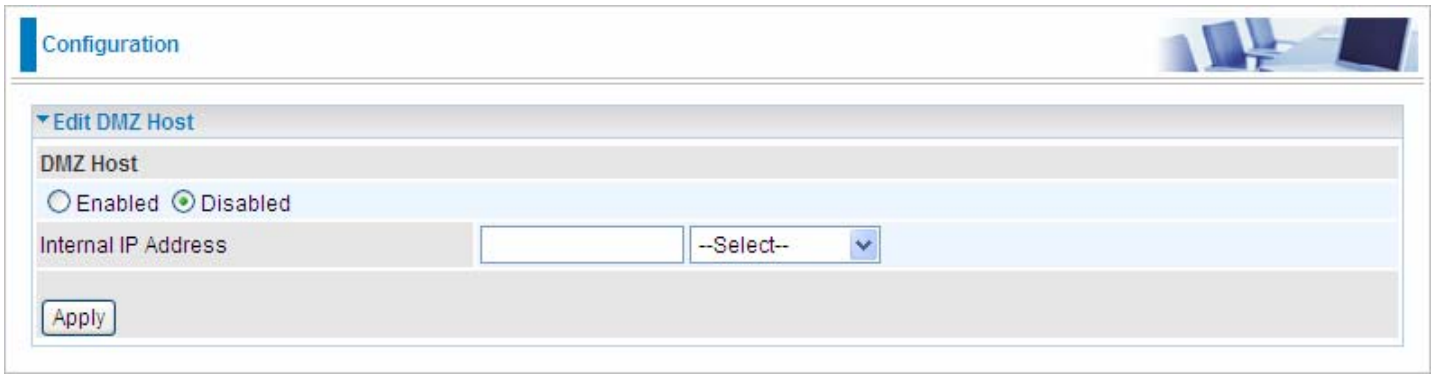
If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

Edit DMZ Host

DMZ Host is a local computer that is exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets especially those that do not use the port number that is being used by any other Virtual Server entries will be checked by the Firewall and NAT algorithms before being passed to the DMZ host.

Cautious: The local computer that is exposed to the Internet may face various security risks.

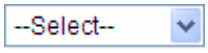
Go to Configuration > Virtual Server > Edit DMZ Host



Enabled: It activates your DMZ function.

Disabled: As set in default setting, it disables the DMZ function.

Internal IP Address: Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.



List all the existing PCs connected to the network. You may assign a PC with an IP address from this list.

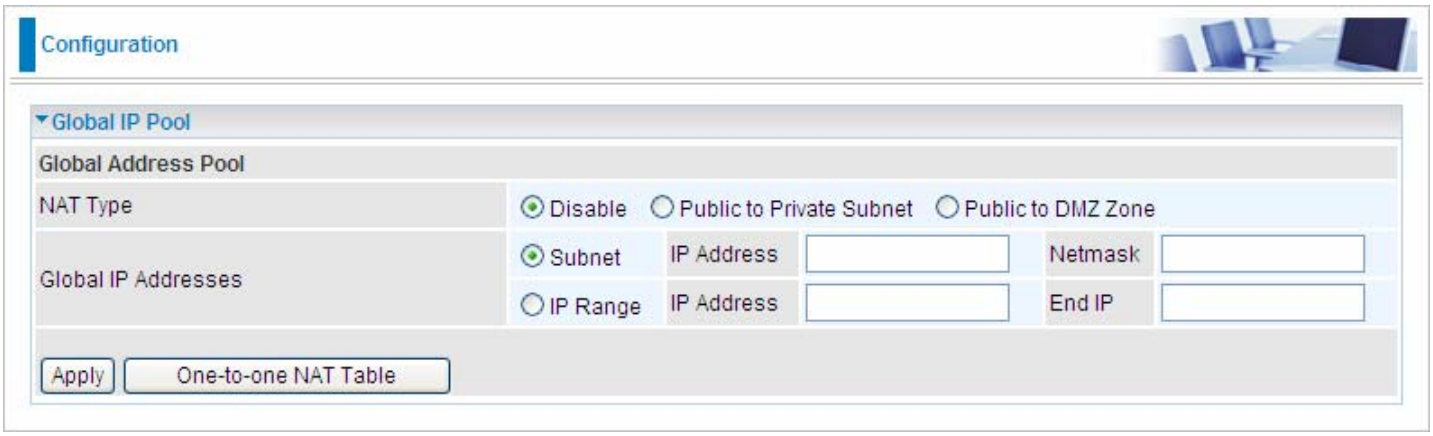
Select the Apply button to apply your changes.

Edit One-to-One NAT (Network Address Translation)

One-to-One NAT maps a specific private / local IP address to a global / public IP address.

If you have multiple public / WAN IP addresses from your ISP, you are eligible to use these IP addresses in One-to-One NAT .

Go to Configuration > Virtual Server > Edit One-to-one NAT



NAT Type: Select the desired NAT type. One-to-One NAT function is set to Disabled by default.

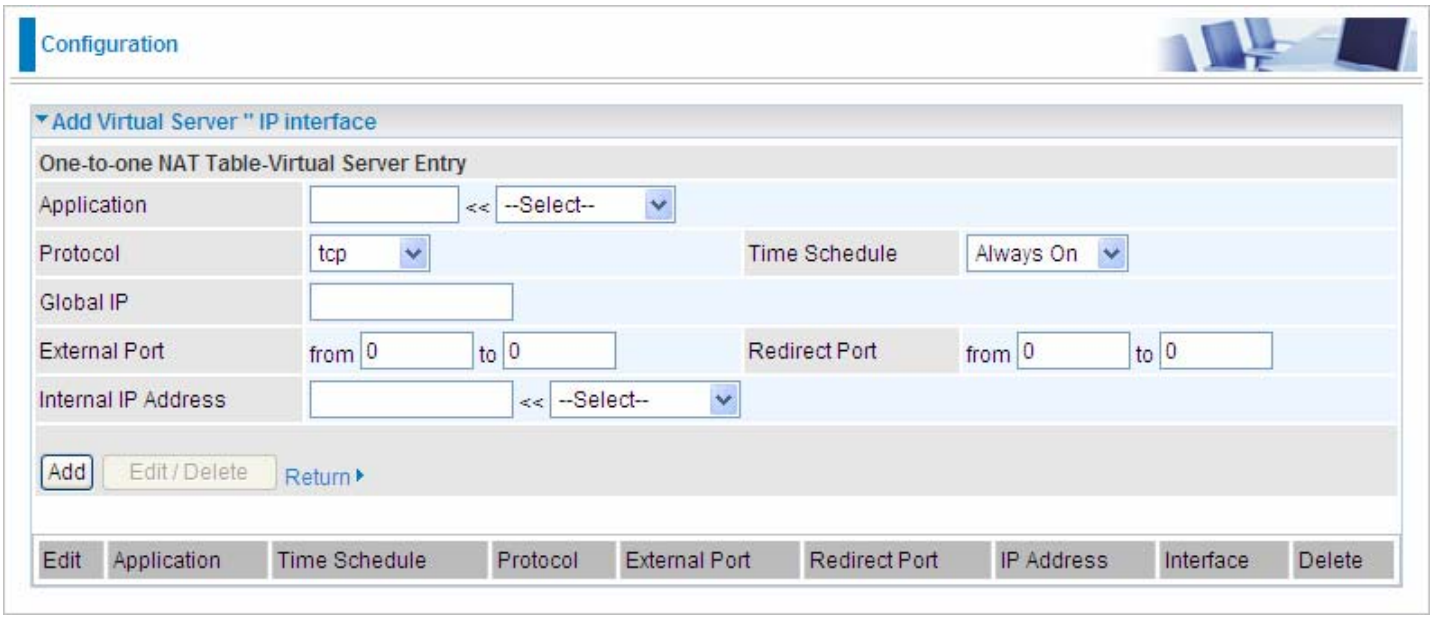
Global IP Address:

Subnet: The subnet of the public/WAN IP address given by your ISP. If your ISP has provided this information, you may insert it here. Otherwise, use IP Range method.

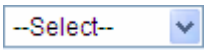
IP Range: The IP address range of your public/WAN IP addresses. For example, IP: 192.168.1.1, end IP: 192.168.1.10

Select the **Apply** button to apply your changes.

Check One-to-one NAT Table to create a new One-to-One NAT rule:



Application: User defined description to identify this entry or click the drop-down menu to select an existing predefined rule.

 **:**20 predefined rules are available. Application, Protocol and External/Redirect Ports will be filled after the selection.

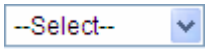
Protocol: It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP.

Time Schedule: User defined time period to enable your virtual server. You may specify a time schedule or select “Always on” for this Virtual Server Entry. For setup and detail, refer to **Time Schedule** section.

Global IP: Define a public / WAN IP address for this Application. This Global IP address must be defined in the Global IP Address blank.

External Port: The Port number on the Remote / WAN side used when accessing the virtual server.

Redirect Port: The Port number used by the Local server in the LAN network.

Internal IP Address: The private IP in the LAN network which provides the virtual server application.  List all the existing PCs connecting to the network. You may assign a PC with an IP address from this list.

Select the **Add** button to apply your changes.

Example: List of some well-known and registered port numbers.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only ports numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports” (Please refer to Table 5). The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic or private ports, are numbered from 49152 through 65535.

For further information, please see IANA’s website at **http://www.iana.org/assignments/port-numbers**

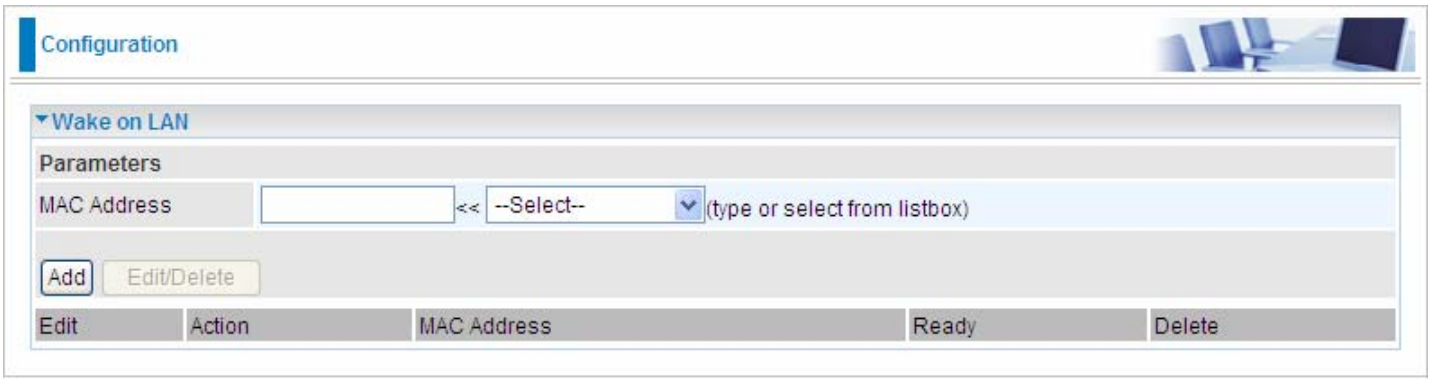
For help on determining which private port numbers are used by common applications on this list, please see the FAQs (Frequently Asked Questions) at **http://www.billion.com**

Table 5: Well-known and registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Contro
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol) / SNTP (Simple Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Wake on LAN

This feature provides greater flexibility for users to turn on / boot the computer of the network from a remotely site.



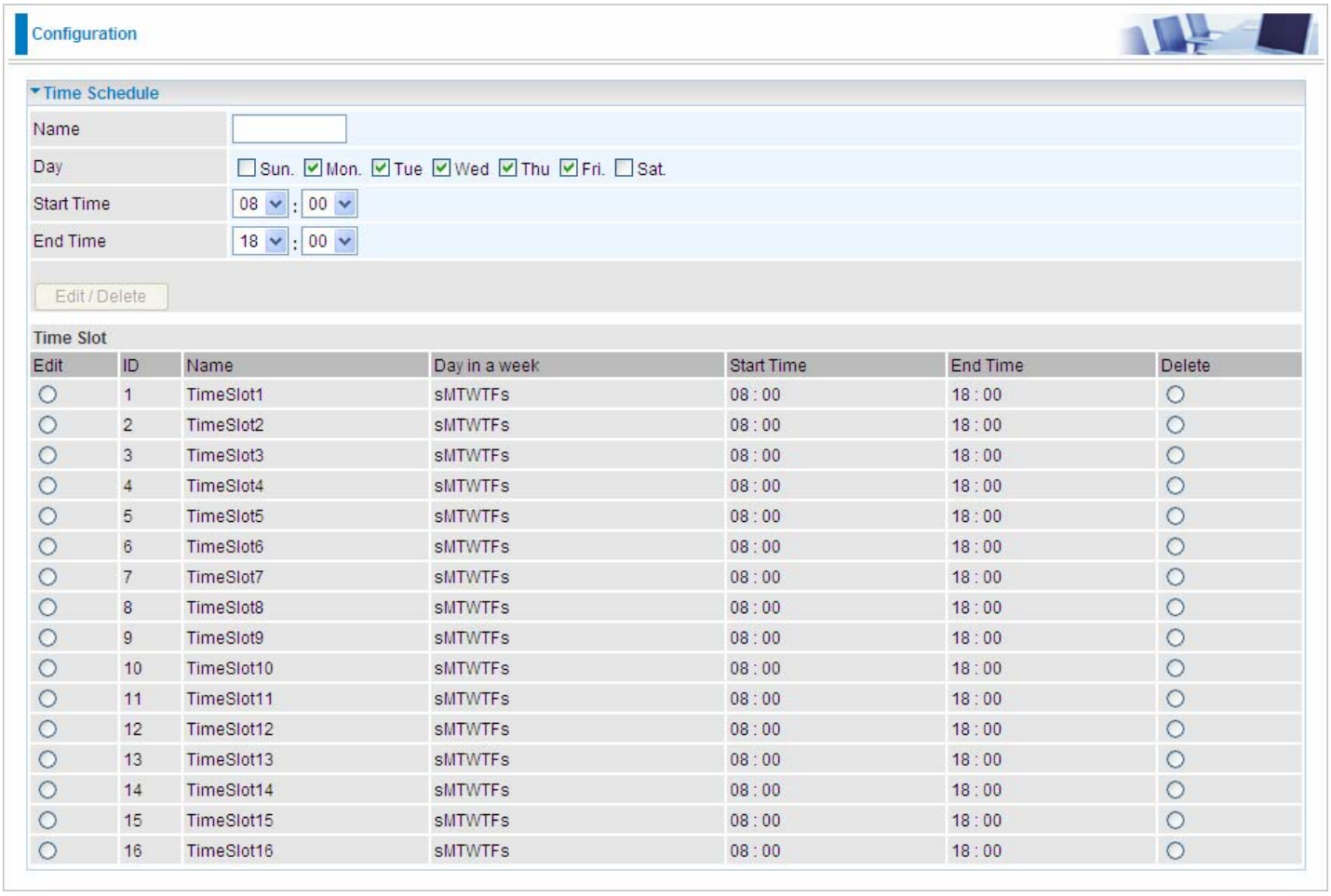
MAC Address: Enter the MAC address of the target computer or you can select the MAC address directly from the Select drop down menu on the right.

--Select--: You can select the MAC from this list.

Time Schedule

The Time Schedule supports up to 16 time slots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allow the use of the Internet by users or applications.

Time Schedule correlates closely with router time. Since router does not have a real time clock on board, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server. Refer to Time Zone for details. Your router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.

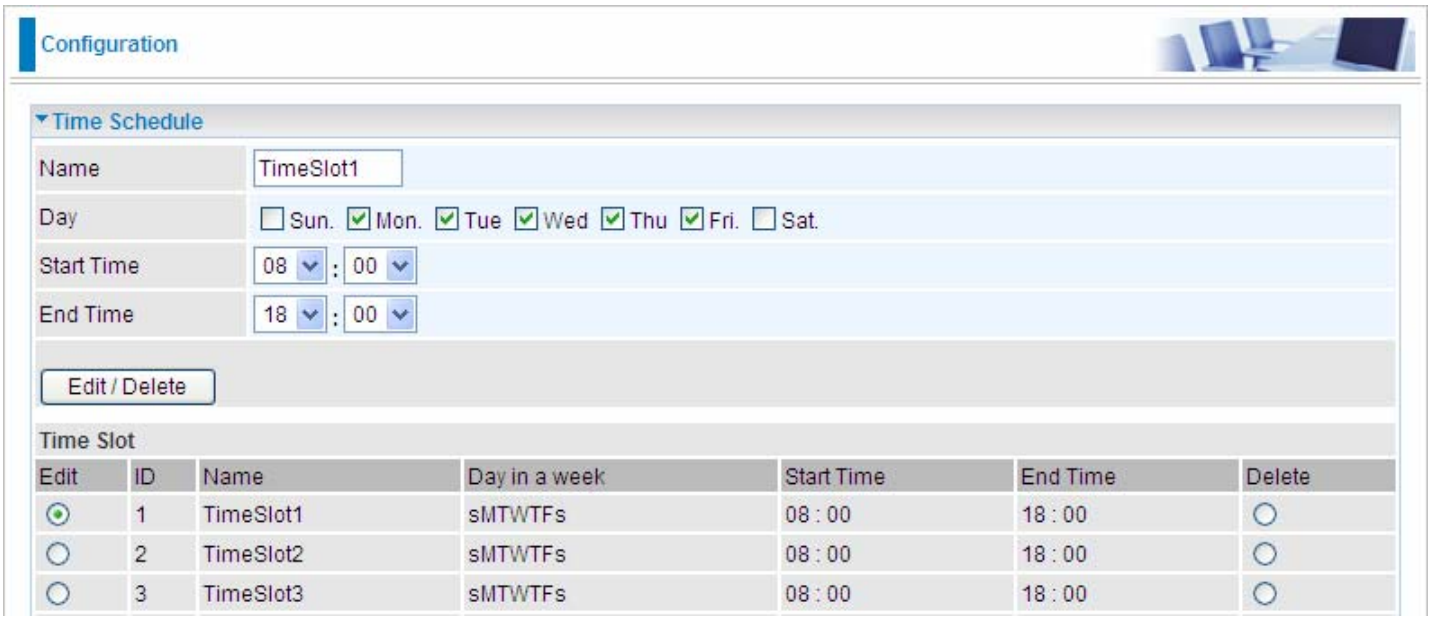


Edit	ID	Name	Day in a week	Start Time	End Time	Delete
○	1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	○
○	2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	○
○	3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	○
○	4	TimeSlot4	sMTWTFs	08 : 00	18 : 00	○
○	5	TimeSlot5	sMTWTFs	08 : 00	18 : 00	○
○	6	TimeSlot6	sMTWTFs	08 : 00	18 : 00	○
○	7	TimeSlot7	sMTWTFs	08 : 00	18 : 00	○
○	8	TimeSlot8	sMTWTFs	08 : 00	18 : 00	○
○	9	TimeSlot9	sMTWTFs	08 : 00	18 : 00	○
○	10	TimeSlot10	sMTWTFs	08 : 00	18 : 00	○
○	11	TimeSlot11	sMTWTFs	08 : 00	18 : 00	○
○	12	TimeSlot12	sMTWTFs	08 : 00	18 : 00	○
○	13	TimeSlot13	sMTWTFs	08 : 00	18 : 00	○
○	14	TimeSlot14	sMTWTFs	08 : 00	18 : 00	○
○	15	TimeSlot15	sMTWTFs	08 : 00	18 : 00	○
○	16	TimeSlot16	sMTWTFs	08 : 00	18 : 00	○

Configuration of Time Schedule

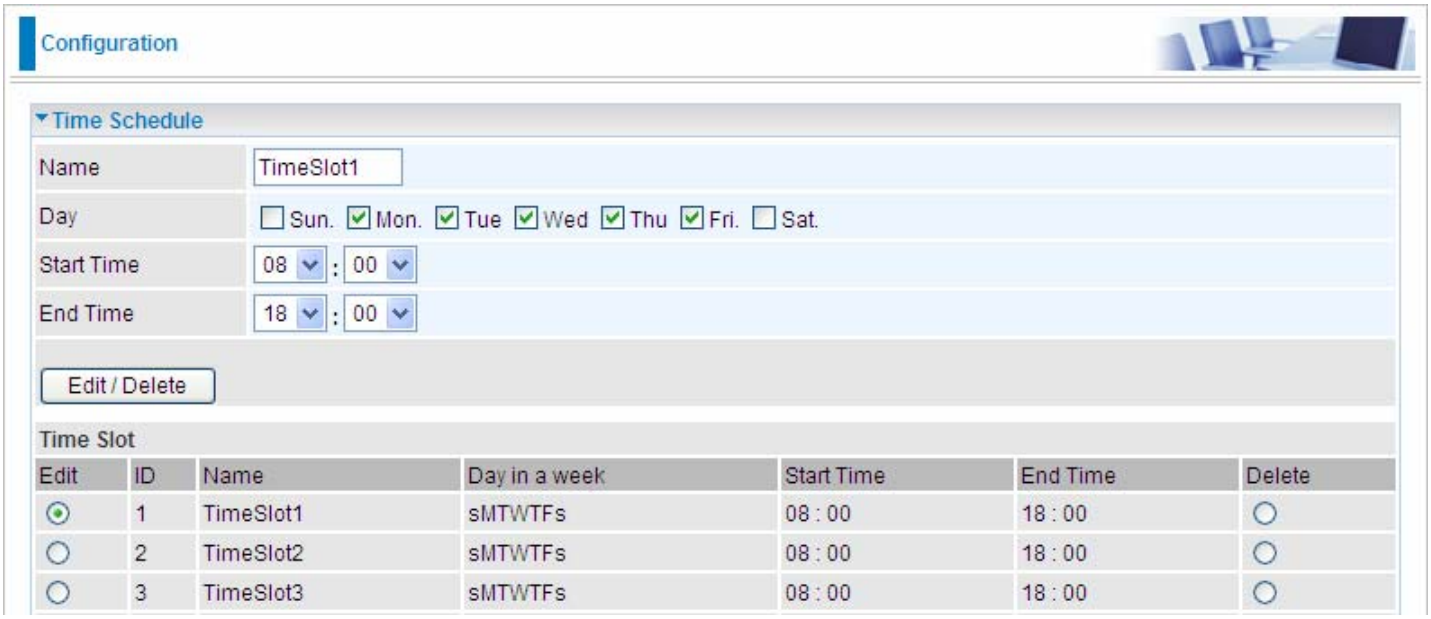
Edit a Time Slot

1. Choose any Time Slot (ID 1 to ID 16) to edit, click Edit radio button.


Configuration
Time Schedule
Name
TimeSlot1
Day
Sun. Mon. Tue Wed Thu Fri. Sat.
Start Time
08 : 00
End Time
18 : 00
Edit / Delete
Time Slot
Edit ID Name Day in a week Start Time End Time Delete
1 TimeSlot1 sMTWTFs 08 : 00 18 : 00
2 TimeSlot2 sMTWTFs 08 : 00 18 : 00
3 TimeSlot3 sMTWTFs 08 : 00 18 : 00

Note: Watch it carefully, the days you have selected will present in capital letter. Lower case letter shows the day(s) is not selected, and no rule will apply on this day(s).

2. A detailed setting of this Time Slot will be shown.


Configuration
Time Schedule
Name
TimeSlot1
Day
Sun. Mon. Tue Wed Thu Fri. Sat.
Start Time
08 : 00
End Time
18 : 00
Edit / Delete
Time Slot
Edit ID Name Day in a week Start Time End Time Delete
1 TimeSlot1 sMTWTFs 08 : 00 18 : 00
2 TimeSlot2 sMTWTFs 08 : 00 18 : 00
3 TimeSlot3 sMTWTFs 08 : 00 18 : 00

ID: This is the index of the time slot.

Name: A user defined description to identify this time portfolio.

Day in a week: The default is set from Monday through Friday. You may also specify the days for the schedule to be applied to.

Start Time: The default is set at 8:00 AM. You may specify the start time of the schedule.

End Time: The default is set at 18:00 (6:00PM). You may specify the end time of the schedule. Choose Edit radio button and click Edit/Delete button to apply your changes.

Delete a Time Slot

Click on the Delete radio button of the Time Slot you wish to delete under the Time Slot section, and then click the Edit/Delete button to confirm the deletion of the selected Time profile, i.e. erase the Day and back to default setting of Start Time / End Time.

Advanced

Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

These are the items within the Advanced section: **Static Route, Static ARP, Dynamic DNS, Device Management, IGMP** and **VLAN Bridge.**

Static Route

Go to Configuration > Advanced > Static Route.

Destination: This is the destination subnet IP address.

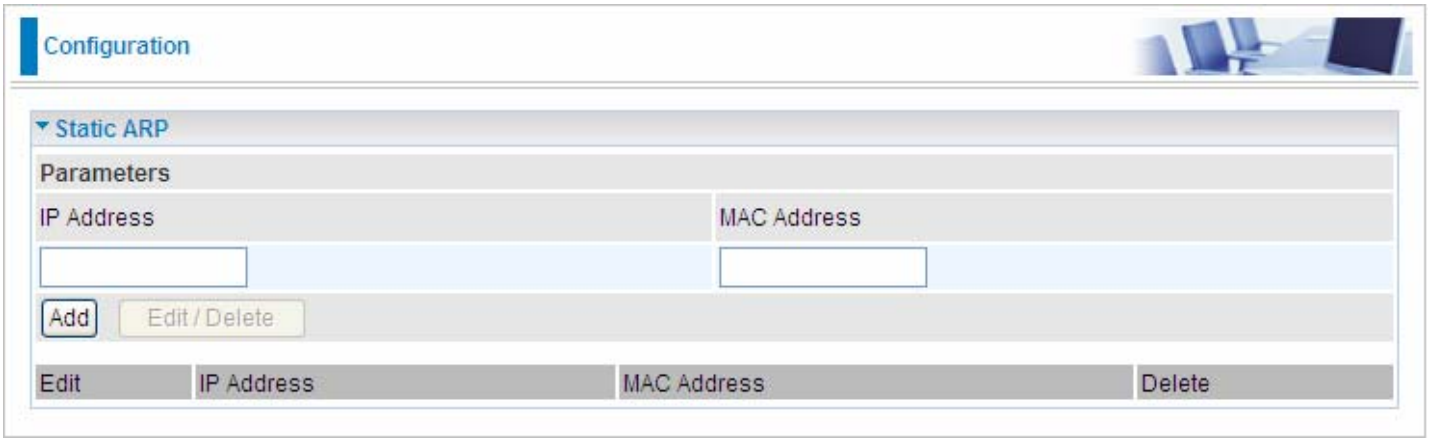
Netmask: Subnet mask of the destination IP addresses based on the above destination subnet IP.

Gateway: This is the gateway IP address to which packets are to be forwarded.

Interface: Select the interface through which packets are to be forwarded.

Cost: This is the same meaning as Hop. This should usually be left at 1.

Static ARP



IP Address: Fill in the IP address of the host computer that is sending the data packet.

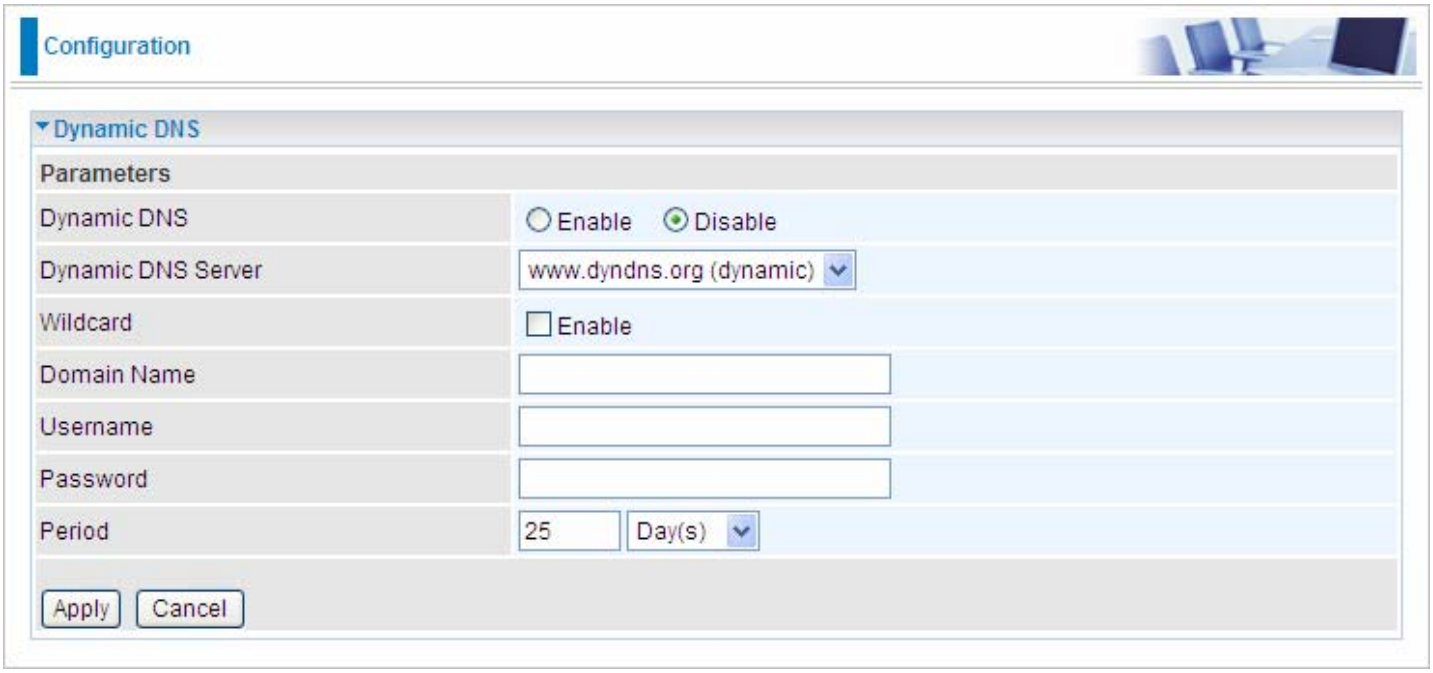
MAC Address: Fill in the MAC address of the computer that the incoming data packets are to be forwarded.

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

You will first need to register and establish an account with the Dynamic DNS provider using their website, for example **http://www.dyndns.org/**

There are more than 5 DDNS services supported.



Dynamic DNS:

Disable: Check to disable the Dynamic DNS function.

Enable: Check to enable the Dynamic DNS function. The following fields will be activated and required.

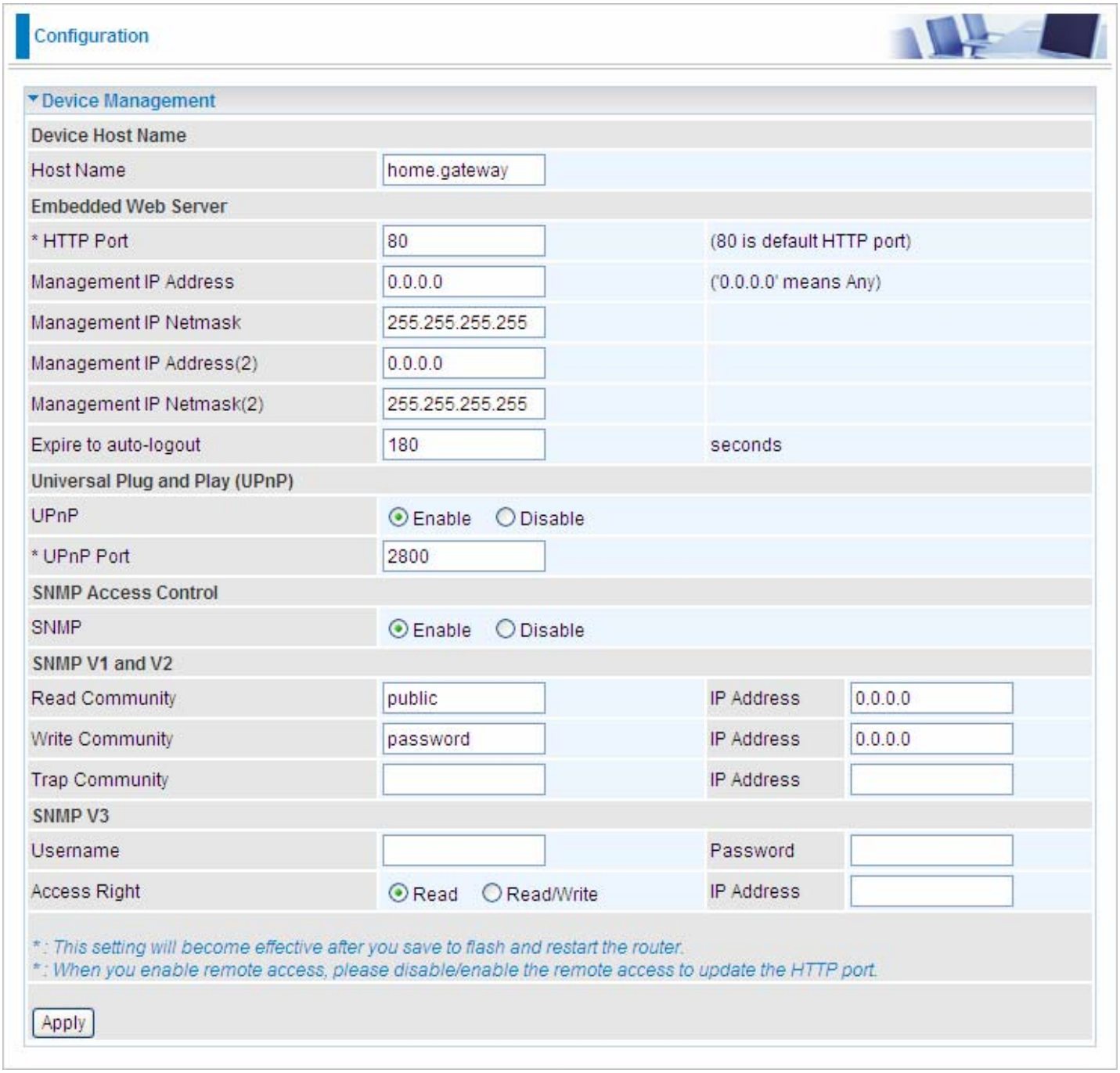
Dynamic DNS Server: Select the DDNS service you have established an account with.

Domain Name, Username and Password: Enter your registered domain name and your username and password for this service.

Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Device Management

The Device Management advanced configuration setting allows you to control your router security option and device monitoring features.



Device Host Name

Host Name: Assign it a name.

Note: The Host Name must have more than a word. These two words should be connected with a '.' period inbetween.

Example:
Host Name: homegateway ==> Incorrect
Host Name: home.gateway or my.home.gateway ==> Correct)

Embedded Web Server (2 Management IP Accounts)

HTTP Port: This is the port number that the router embedded web server (for web-based configuration) will use. The default value is the standard HTTP port 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Management IP Address: You may specify an IP address for logon and access the router web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

Expire to auto-logout: Specify a duration for the system to log the user out of the configuration session automatically.

For Example:

User A changes the HTTP port number to 100, specifies their own IP address as 192.168.1.55 and sets the logout time as 100 seconds. The router will only allow User A to access the Web GUI from the IP address 192.168.1.55 by typing **http://192.168.1.254:100** in their web browser. Nevertheless, after 100 seconds the device will automatically log User A out of the system.

Universal Plug and Play (UPnP)

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer featuers between devices. UPnP offers many advantages for users that run NAT routers through UPnP NAT Traversal and on supported systems. This makes tasks such as port forwarding become easier by letting the application control the required settings & remove the need for the user to control the advanced configuration of their device.

Both operating system and the relevant application must support UPnP in addition to the router. Windows XP and Windows ME natively support UPnP (when the component is installed) while Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to gain support for UPnP. Nevertheless Windows 2000 does not support UPnP.

Disable: Check to disable the router's UPnP functionality.

Enable: Check to enable the router's UPnP functionality.

UPnP Port: Its default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports already being used, you may wish to change the port.
SNMP Access Control (Software on a PC within the LAN is required in order to utilize this function) – Simple Network Management Protocol.

- **Disable:** Check to disable the router's SNMP functionality.

- **Enable:** Check to enable the router's SNMP functionality.

SNMP Access Control (Software on a PC within the LAN is required in order to utilize this function) – Simple Network Management Protocol.

SNMP V1 and V2:

Read Community: Specify a name to be identified as the Read Community and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user with this IP address will be able to view the data.

Write Community: Specify a name to be identified as the Write Community and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users with this IP address will be able to view and modify the data.

Trap Community: Specify a name to be identified as the Trap Community and an IP address. This community string will be checked against the string entered in the configuration file. Once the

string name is matched, users with this IP address will be sent SNMP Traps.

SNMP V3:

Specify a name and password for authentication and define the access right from an identified IP address. Once the authentication has succeeded, users with this IP address will be able to view and modify the data.

SNMP Version: SNMPv2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The “c” comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for “security”, but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II) System group

System group

Interface group

Address Translation group

IP group

ICMP Group

TCP group

UDP group

EGP (not applicable)
Transmission
SNMP group

From RFC 1650 (EtherLike-MIB)

dot3stats

From RFC 1493 (Bridge MIB)

dot1 dBase group

dot1 dTp group

dot1 dStp group (if configured as spanning tree)

From RFC 1472 (PPP/Security MIB)

PPP security group

From RFC 1473 (PPP/IP MIB)

PPP IP group

From RFC 1474 (PPP/Bridge MIB)

PPP Bridge group

From RFC 1573 (IfMIB)

ifMIBObjects group

From RFC 1695 (atmMIB)

atmMIBObjects

From RFC 1907 (SNMPv2)

only snmpSetSerialNo OID

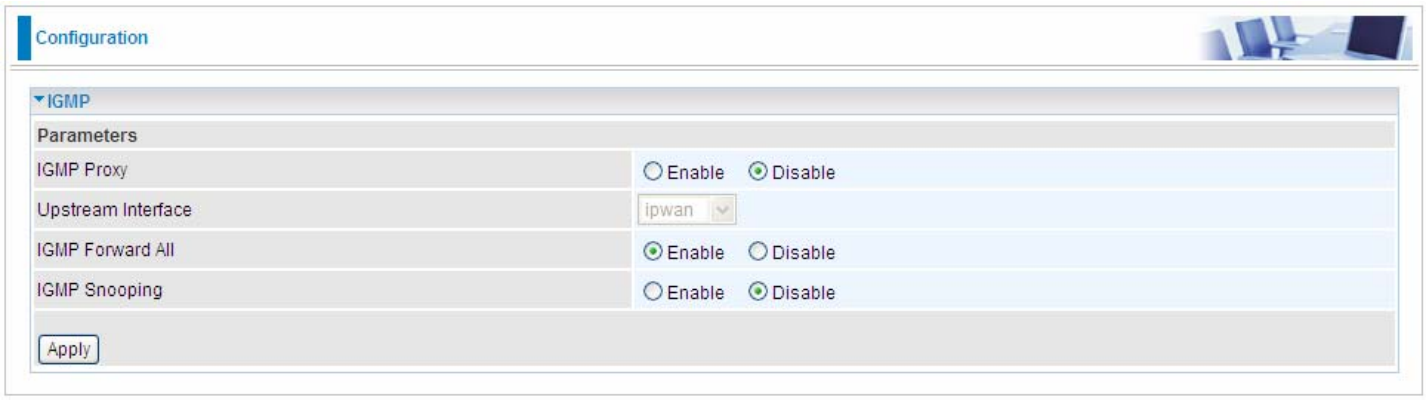
From RFC 1471 (PPP/LCP MIB)

pppLink group

pppLgr group (not applicable)

IGMP

IGMP, known as Internet Group Management Protocol, is used to manage hosts from multicast group.



IGMP Proxy: Enables or disables the router's IGMP Proxy.

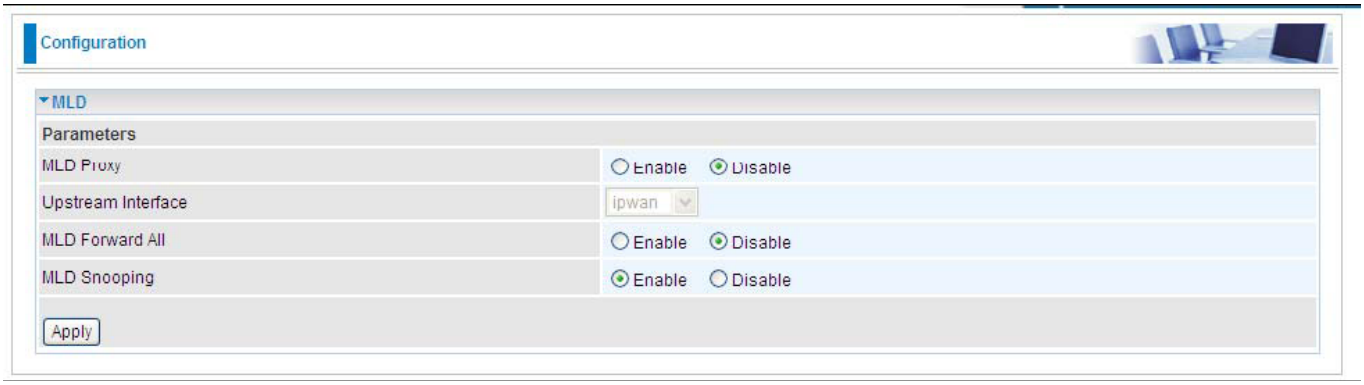
Upstream Interface: When IGMP Proxy enabled, sets one of the router's existing IP interfaces as the upstream interface; all other router interfaces are designated downstream interfaces.

IGMP Forward All: Enables/Disables your router's ability to forward multicast traffic to ALL interfaces.

IGMP Snooping: Enables/Disables the IGMP Snoop functionality in the bridge. When the IGMP snoop functionality is enabled, all the attached bridge interfaces are designated as downstream interfaces.

MLD

MLD, short for **Multicast Listener Discovery** protocol, is a component if the Internet Protocol version 6(IPv6) suite. MLD is used by IPv6 to discover multicast listeners on a directly attached link, much as IGMP used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.



MLD Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients and forwards it to the router after some dealings. Support MLDv1 and MLDv2.

Upstream Interface: When MLD Proxy enabled, sets one of the router's existing IP interfaces as the upstream interface; all other router interfaces are designated downstream interfaces.

MLD Forward All: select enable to forward the multicast packets to all ports. If select disable, the multicast packets will be forwarded to ports set according to the MLD Snooping below.
MLD Snooping: similar to IGMP snooping, listens in on the MLD conversation between hosts and routers by processing MLD packets sent in a multicast network, and it analyzes all MLD packets between hosts and the connected multicast routers in the network. Without MLD snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With MLD snooping, multicast traffic of a group is only forwarded to ports that have members of that group.

VLAN Bridge

VLAN (Virtual Local Area Network) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment.

Edit: Edit your member ports in selected VLAN group.

Create VLAN: To create another VLAN group.

Logout

To exit the router web interface, choose Logout. Please save your configuration setting before logging out of the system.

Be aware that the router configuration interface can only be accessed by one PC at a time. Therefore when a PC has logged into the system interface, the other users cannot access the system interface until the current user has logged out of the system. If the previous user forgets to logout, the second PC can only access the router web interface after a user-defined auto logout period which is by default 3 minutes. You can however modify the value of the auto logout period using the Advanced > Device Management section of the router web interface. Please see the Advanced section of this manual for more information.

Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

Problems with the router

Problem	Suggested Action
None of the LEDs lit when the router is turned on.	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router more than 6 seconds.

Problems with WAN interface

Problem	Suggested Action
Initialization of ADSL connection (line- sync) fail	Make sure that the telephone cable is properly connected between the ADSL port and the wall jack. The ADSL LED on the front panel should lit. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router GE. If you still have problem, you may need to verify these settings with your ISP.
Frequent loss of ADSL linesync (disconnection)	Make sure that all devices (e.g telephone, fax machine, analogue modems) that are connected to the telephone line as your router have a line filter connected between them and the wall outlet (unless your are using a Central Splitter or Central Filter installed by a qualified and licensed electrician). Make sure that all line filters are correctly installed as missing line filters or incorrect installation of line filters can cause ADSL connection problem, including frequent disconnections.

Problem with LAN interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, and check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

Appendix: Product Support & Contact

Following the suggestions listed in the Troubleshooting section of the user manual can help you solve most of your problems. However if your problems persist or you come across other technical issues that are not listed in the Troubleshooting section, please contact the dealer from where you purchased your product.

Contact Billion

Worldwide:

http://www.billion.com

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 98, Windows NT, Windows 2000, Windows Me, Windows XP, Windows Vista and Windows 7 are registered Trademarks of Microsoft Corporation.